Grupo BeIT

NEWSLETTER

Blog CEO

Riesgo reputacional y financiero ante un ciberataque

Noticia BeIT

Caída AWS

Edición 48

¿Tu entorno cloud está a prueba de persistencia?

Servicios BeIT

Ethical Hacking

ELIT INFRASTRUCTURE SERVICES

BURÖMC SEGURIDAD INFORMÁTICA

Edición 48

Riesgo reputacional y financiero ante un ciberataque

Por: Elías Cedillo, Fundador y CEO GrupoBeIT

Durante 2025, el fenómeno del phishing ha alcanzado un punto de madurez que redefine su papel dentro del panorama del cibercrimen. Lo que antes era un intento aislado de engañar a usuarios mediante correos electrónicos mal redactados, se ha transformado en una operación criminal industrializada, organizada y profesional. Este cambio se debe, principalmente, a la aparición del modelo conocido como Phishing-as-a-Service (PhaaS), un sistema que replica las ventajas del software legítimo como servicio (SaaS), pero aplicado al fraude digital.

El PhaaS permite que ciberdelincuentes sin amplios conocimientos técnicos contraten una suscripción mensual o por campaña y obtengan acceso a toda la infraestructura necesaria para ejecutar ataques masivos: plantillas realistas de sitios web falsos, herramientas de envío automatizado, servicios de alojamiento encubiertos y paneles de control para gestionar víctimas y resultados. Este modelo representa un cambio estructural en la economía del delito, porque reduce drásticamente las barreras de entrada, aumenta la escala de operación y ofrece un retorno de inversión inmediato para los atacantes. En términos simples, el phishing ya no requiere de un hacker experto: basta con una tarjeta de criptomonedas y acceso a una de estas plataformas.

Los informes de seguridad más recientes confirman la magnitud de este cambio. Durante los primeros meses de 2025, distintas empresas del sector detectaron un crecimiento sostenido de campañas originadas en servicios PhaaS. Plataformas como Caffeine, EvilProxy y Greatness —conocidas en la comunidad de ciberinteligencia— ofrecen portales con interfaces gráficas intuitivas, registro automatizado y soporte técnico incluido. De acuerdo con reportes globales, entre un 60% y un 70% de los ataques de phishing actuales pueden vincularse con servicios de este tipo, lo que demuestra que el modelo de suscripción criminal se ha consolidado como estándar en la cadena de fraude digital.

A diferencia del phishing tradicional, que dependía de correos genéricos y errores gramaticales notorios, el phishing moderno se apoya en inteligencia artificial y automatización para personalizar mensajes, adaptar el lenguaje al contexto de la víctima e imitar de manera casi perfecta a marcas y servicios de confianza. Esto ha llevado a un incremento en la tasa de éxito de los ataques, especialmente en sectores financieros, corporativos y de tecnología, donde la presión de tiempo y la sobrecarga de comunicación facilitan el descuido humano.

En 2025 también se consolidaron nuevas tácticas dentro de las campañas de phishing. Una de las más visibles es el "*quishing*", o uso de códigos QR maliciosos que redirigen a sitios falsos. Esta técnica aprovecha el hábito extendido de escanear códigos en restaurantes, eventos o documentos corporativos, ocultando direcciones URL manipuladas que son difíciles de identificar visualmente. Otra tendencia preocupante son los **ataques a los sistemas de autenticación multifactor (MFA)**. Los delincuentes utilizan kits de intermediación (conocidos como *Adversary-in-the-Middle*) que interceptan tokens de autenticación o sesiones activas, logrando burlar incluso configuraciones avanzadas de seguridad. Casos documentados muestran que campañas completas de PhaaS ya incorporan módulos para capturar códigos de un solo uso o explotar el fenómeno del "MFA fatigue", en el que el usuario aprueba inadvertidamente una solicitud de acceso repetitiva.

Además, la **suplantación de marcas de confianza** ha alcanzado un nivel sin precedentes. Los servicios PhaaS ofrecen catálogos de plantillas que replican visualmente portales de bancos, empresas de logística, plataformas de firma digital o aplicaciones de productividad. Esto permite que las campañas se personalicen por idioma, región e incluso por dispositivo, aumentando la credibilidad de la trampa. Sumado a ello, muchos atacantes alojan sus sitios fraudulentos dentro de servicios legítimos en la nube, lo que complica la detección y reduce la eficacia de los bloqueos automáticos.

El impacto para las organizaciones es profundo. Ya no basta con filtrar correos sospechosos o capacitar a los empleados en la detección de mensajes fraudulentos. Las nuevas campañas combinan múltiples canales —correo, mensajería instantánea, redes sociales, SMS e incluso entornos físicos— para lograr su objetivo. Los equipos de seguridad deben integrar capacidades de detección basadas en comportamiento, protección de identidad, endurecimiento de MFA y monitoreo continuo de dominios falsos. De igual forma, la dirección ejecutiva debe entender que el phishing ha pasado de ser un problema de "usuarios descuidados" a una amenaza estratégica que puede comprometer accesos privilegiados, sistemas financieros y la confianza de los clientes.

El auge del PhaaS simboliza una transición más amplia: el crimen digital se ha convertido en un ecosistema empresarial, con estructuras jerárquicas, especialización, soporte y modelos de negocio sostenibles. La economía del fraude opera ahora con la misma lógica que la economía legítima de servicios en la nube: escalabilidad, automatización y disponibilidad bajo demanda. En consecuencia, la defensa debe evolucionar a la misma velocidad, combinando tecnología avanzada, inteligencia de amenazas compartida y programas de concientización adaptados a este nuevo contexto.

En definitiva, 2025 marca el año en que el phishing dejó de ser simplemente un ataque para convertirse en un **servicio profesionalizado**, disponible para cualquiera que quiera alquilarlo. El desafío ya no es evitar que los correos maliciosos lleguen, sino **detectar, contener y responder** a una industria del engaño que funciona en la nube, con soporte 24/7 y un modelo de suscripción. La resiliencia digital de las organizaciones dependerá, cada vez más, de su capacidad para anticiparse a esta nueva economía del crimen.

Fuentes y referencias

- Trustwave. *Phishing-as-a-Service (PhaaS): A Cybercrime Subscription Service.*
- Barracuda Networks. *Everything You Need to Know About Phishing-as-a-Service (2025).*
- Barracuda Networks. *Threat Spotlight: Phishing-as-a-Service — A Fast-Evolving Threat (Mar 2025).*
- The Hacker News. *17,500 Phishing Domains Target 316 Brands in 74 Countries (Sept 2025).*
- SEKOIA.IO. *Global Analysis of Adversary-in-the-Middle Phishing Threats (2025).*
- Kela Cyber Intelligence. *Phishing-as-a-Service: How It Works and Why It's Booming (2025).*
- CrowdStrike. *Global Threat Report 2025.*
- Sophos. *Active Adversary Report 2025.*
- Bitdefender. *Cybersecurity Assessment and Threat Landscape 2025.*
- Kaspersky. *Phishing and Scam Statistics Q2 2025.*

Panorama Global

Caída de AWS

NOTICIA BeIT

El 20 de octubre de 2025 comenzó como cualquier otro día para millones de usuarios y empresas en todo el mundo, pero lo que muchos experimentaron fue un sobresalto: plataformas comunes dejaron de funcionar, juegos se congelaron, asistentes de voz no respondieron y medios de pago se interrumpieron. La causa principal se encontró en uno de los pilares invisibles de la nube moderna: la infraestructura de Amazon Web Services (AWS) en su región más crítica, US-EAST-1 (Virginia). Según el propio AWS, no fue un ataque sofisticado ni un error humano directo, sino una falla en uno de sus sistemas de automatización de DNS (Domain Name System) que desencadenó un efecto dominó en otros servicios.

El proceso se desarrolló de la siguiente forma: una automatización llamada “DNS Planner” generó un plan de actualización para los registros DNS que usa otro sistema llamado “DNS Enactor”. Debido a una condición de carrera —cuando dos sistemas automáticos actúan casi simultáneamente sin la sincronización adecuada—, uno de ellos aplicó por error una versión antigua del plan, borrando registros válidos y dejando campos vacíos. En particular, el registro DNS para el servicio Amazon DynamoDB quedó en blanco, lo que provocó que miles de otros servicios internos de AWS, y por extensión muchos servicios externos, ya no encontraran a dónde enviar sus peticiones.

Ese fallo interno, aparentemente pequeño, generó un daño tan profundo porque muchos componentes críticos del ecosistema de AWS dependían de DynamoDB o de los sistemas afectados por la automatización DNS. Cuando DynamoDB dejó de resolver correctamente, otros sistemas como las instancias de cómputo (EC2), la gestión de cargas, los balanceadores de red y las funciones sin servidor (Lambda) empezaron a experimentar fallos. La cascada afectó desde servicios de pago y banca hasta videojuegos y dispositivos de hogar inteligente. Plataformas globales como Snapchat, Fortnite, Alexa e incluso cámaras de seguridad conectadas a internet reportaron interrupciones.

Desde el punto de vista de AWS, la interrupción se manifestó primero como un aumento de latencias y errores en múltiples servicios en la región US-EAST-1, y oficialmente se resolvió el problema del DNS a las 2:24 a.m. PDT, con todos los servicios anunciados como normales nuevamente alrededor de las 6:01 p.m. ET ese mismo día. Aunque el núcleo del fallo se corrigió en unas horas, la recuperación completa requirió más tiempo debido al gran número de peticiones pendientes y a la necesidad de reactivar ciertos subsistemas que habían sido temporalmente limitados para estabilizar la plataforma.

Para evitar que un incidente similar vuelva a ocurrir, AWS adoptó una serie de medidas: desactivó temporalmente las automatizaciones implicadas —DNS Planner y DNS Enactor— mientras realiza revisiones del código, añadió mecanismos que impidan que una versión obsoleta del plan de DNS sobrescriba la vigente, reforzó las pruebas internas de máquinas virtuales y control de tráfico, y revisó sus procesos de recuperación para mejorar los tiempos de respuesta ante fallos futuros. Estas acciones apuntan a fortalecer la resiliencia de su infraestructura y reducir la posibilidad de fallos sistémicos derivados de automatizaciones descoordinadas.

El impacto de este evento fue profundo, porque puso en evidencia la fragilidad inherente de la dependencia de una sola región o proveedor de nube. Incluso las arquitecturas multicapa, con zonas de disponibilidad múltiples, sufrieron el golpe, ya que muchas dependencias de control, autenticación o infraestructura global apuntaban todavía a US-EAST-1. Analistas del sector señalaron que el hecho de que esa región siga siendo el "cerebro" de muchos servicios globales hace que un fallo localizado pueda tener un efecto planetario. Para las empresas, la lección es clara: usar múltiples regiones, múltiples proveedores, diseñar para el fallo y automatizar la conmutación por error no es solo una buena práctica, sino una necesidad esencial para garantizar continuidad operativa.

En resumen, lo ocurrido con AWS en octubre de 2025 es un recordatorio de que, aunque la nube parece interminable y ubicua, su operación depende de sistemas internos complejos y automatizados que pueden fallar. No fue un error humano directo ni un ciberataque: fue un fallo de automatización, pero con consecuencias globales. Se solucionó mediante la identificación de la causa raíz, la desactivación temporal de los sistemas implicados, la revisión del código, la implementación de controles adicionales y la mejora de los procesos de recuperación. Para las organizaciones que dependen de la nube, la moraleja es que la resiliencia no es un beneficio adicional, sino una condición básica. Prepararse para el fallo hoy es lo que garantiza que el servicio siga funcionando mañana.

Fuentes y referencias

- **20minutos**. “Caída de AWS: fallo no humano por automatización DNS.”
- **ThousandEyes (Cisco)**. “AWS Outage Analysis — October 2025.”
- **About Amazon / AWS Service Updates**. “Post-incident summary: US-EAST-1 DNS disruption.”
- **The Verge**. “Major AWS outage took down Fortnite, Alexa, Snapchat, and more.”
- **The Register**. “US-EAST-1: The AWS brain that makes the internet tremble.”
- **Akamai Technologies**. “Understanding DNS automation failures in hyperscale environments.”
- **Omdia Research**. “Cloud concentration risk: The AWS outage and what it teaches enterprises.”

¿Tu entorno cloud está a prueba de persistencia?

En la actualidad, la adopción de la nube se ha consolidado como una de las decisiones estratégicas más relevantes para la competitividad empresarial. La flexibilidad, escalabilidad y eficiencia que ofrece han transformado la manera en que las organizaciones operan, almacenan y procesan información. Sin embargo, esta misma transformación ha abierto un nuevo frente de riesgo: la persistencia de las amenazas dentro de los entornos cloud. La pregunta que cada ejecutivo debería hacerse hoy no es si su infraestructura en la nube está segura, sino si está preparada para resistir la persistencia de un atacante una vez que ha logrado acceder.

En el ámbito de la ciberseguridad, la persistencia se entiende como la capacidad que tiene un actor malicioso de mantener el acceso dentro de un sistema comprometido durante un periodo prolongado, incluso frente a intentos de remediación o limpieza. En entornos cloud, esta capacidad se potencia debido a la naturaleza dinámica de los recursos, la automatización de procesos y la complejidad de los entornos híbridos y multicloud. Los atacantes no necesitan ya controlar un servidor físico; basta con comprometer credenciales, servicios de automatización o roles privilegiados para establecer puntos de reingreso invisibles que se activan incluso después de una aparente recuperación.
Un factor que agrava el problema es la falsa sensación de seguridad que muchas empresas asumen al migrar a la nube. Confiar plenamente en el modelo de responsabilidad compartida sin entender sus límites puede dejar grietas considerables. Los proveedores cloud protegen la infraestructura subyacente, pero la configuración, la gestión de accesos, las identidades y las aplicaciones siguen siendo responsabilidad del cliente. Esto significa que una política IAM (Identity and Access Management) mal diseñada, un rol con privilegios excesivos o una API expuesta pueden servir como puerta de entrada para la persistencia de amenazas.

La sofisticación de los ataques actuales se refleja en cómo los adversarios aprovechan las propias herramientas y servicios cloud para camuflar su actividad. Es común que utilicen funciones nativas, como lambdas o scripts de automatización, para reinstalar cargas maliciosas o exfiltrar información sin levantar sospechas. También pueden manipular logs, alterar flujos de CI/CD o incluso crear recursos “fantasma” que persisten en el tiempo. En muchos casos, las soluciones tradicionales de detección no logran identificar estas acciones porque las perciben como operaciones legítimas dentro del entorno.

Desde una perspectiva estratégica, abordar la persistencia requiere un cambio de paradigma: pasar de una seguridad reactiva a una seguridad basada en resiliencia y visibilidad continua. Esto implica que las organizaciones deben tener no solo mecanismos de protección, sino también capacidades avanzadas de detección y respuesta orientadas específicamente al contexto cloud. La implementación de herramientas como Cloud Security Posture Management (CSPM), Cloud Workload Protection Platforms (CWPP) o Cloud Detection and Response (CDR) se vuelve indispensable para obtener trazabilidad, identificar anomalías en tiempo real y reducir los tiempos de permanencia de un atacante.

La gobernanza también juega un papel determinante. Las empresas deben establecer políticas de segmentación y control de accesos basadas en el principio de privilegio mínimo, junto con una gestión rigurosa de identidades humanas y no humanas. Un enfoque Zero Trust adaptado al entorno cloud es hoy una exigencia, no una tendencia. Además, la educación continua de los equipos técnicos y ejecutivos es fundamental, ya que la persistencia muchas veces se apoya en errores humanos, configuraciones inadecuadas o una falta de cultura de seguridad en la toma de decisiones operativas.

Por otra parte, la integración de inteligencia de amenazas y la correlación de datos entre entornos on-premise y cloud son factores clave para anticipar comportamientos maliciosos. La persistencia no se limita a un ataque puntual; suele ser parte de campañas prolongadas, donde los atacantes estudian los flujos de la organización y actúan con precisión quirúrgica. Detectar patrones, correlacionar eventos y aplicar aprendizaje automático sobre grandes volúmenes de telemetría permite identificar indicios de persistencia incluso antes de que el daño sea evidente.

En última instancia, la pregunta sobre si un entorno cloud está a prueba de persistencia no tiene una respuesta simple ni definitiva. La verdadera fortaleza de una organización no radica en evitar todos los incidentes, sino en su capacidad para resistir, adaptarse y recuperarse rápidamente ante ellos. Las empresas que entienden la persistencia como una amenaza sistémica, y no como un incidente aislado, serán las que logren construir entornos más seguros, sostenibles y resilientes frente a un panorama de amenazas en constante evolución.

Fuentes y referencias

- Gartner, *Market Guide for Cloud Detection and Response*, 2025.
- IBM Security, *X-Force Threat Intelligence Index 2025*.
- Palo Alto Networks, *Unit 42 Cloud Threat Report, 2H 2025*.
- CrowdStrike, *Global Threat Report 2025*.
- Microsoft, *Cyber Signals: Securing Identities in the Cloud Era*, 2025.

Google Cloud, *Threat Horizons Report*, 2025.

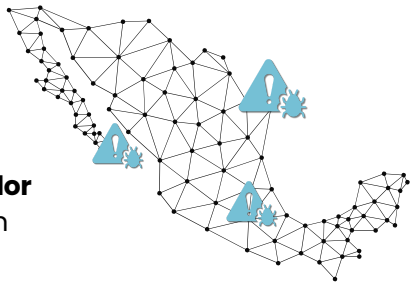
BURÓMC SEGURIDAD INFORMÁTICA

Grupo BeIT

ELIT INFRASTRUCTURE SERVICES

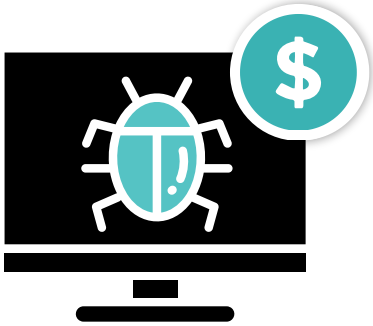
ETHICAL HACKING MODULAR

¿Sabías que?



México
Solo en el primer trimestre de 2025 **México recibió alrededor de 35,200 millones de intentos de ciberataques,** según un informe de Fortinet.

El costo del cibercrimen en México alcanzaría los **105,000 millones de dólares en 2025.**



Solo el 20% de las organizaciones está preparada para enfrentar un ciberataque, según un informe de Deloitte.

Según Alianza Nacional de Inteligencia Artificial México, **7 de cada 10** pequeñas y medianas empresas que sufren un ciberataque quiebran.

La falta de análisis de vulnerabilidades, pruebas de penetración, monitoreo de la Dark Web, revisión de código o evaluación de rendimiento puede estar costándole a tu empresa mucho más de lo que imaginas.

¡Agendemos una cita!

Contáctanos

ETHICAL HACKING

Para más información o una propuesta a la medida, comunícate o contesta directamente a este correo.
Nota: Aplican términos y condiciones. Precio sujeto a dimensionamiento de cada proyecto.

+52 56 5100 8613

admmarketing@buromc.com