Según hallazgos de Palo Alto Networks Unit 42, ciberdelincuentes están explotando entornos de AWS para distribuir campañas de phishing dirigidas a víctimas desprevenidas.

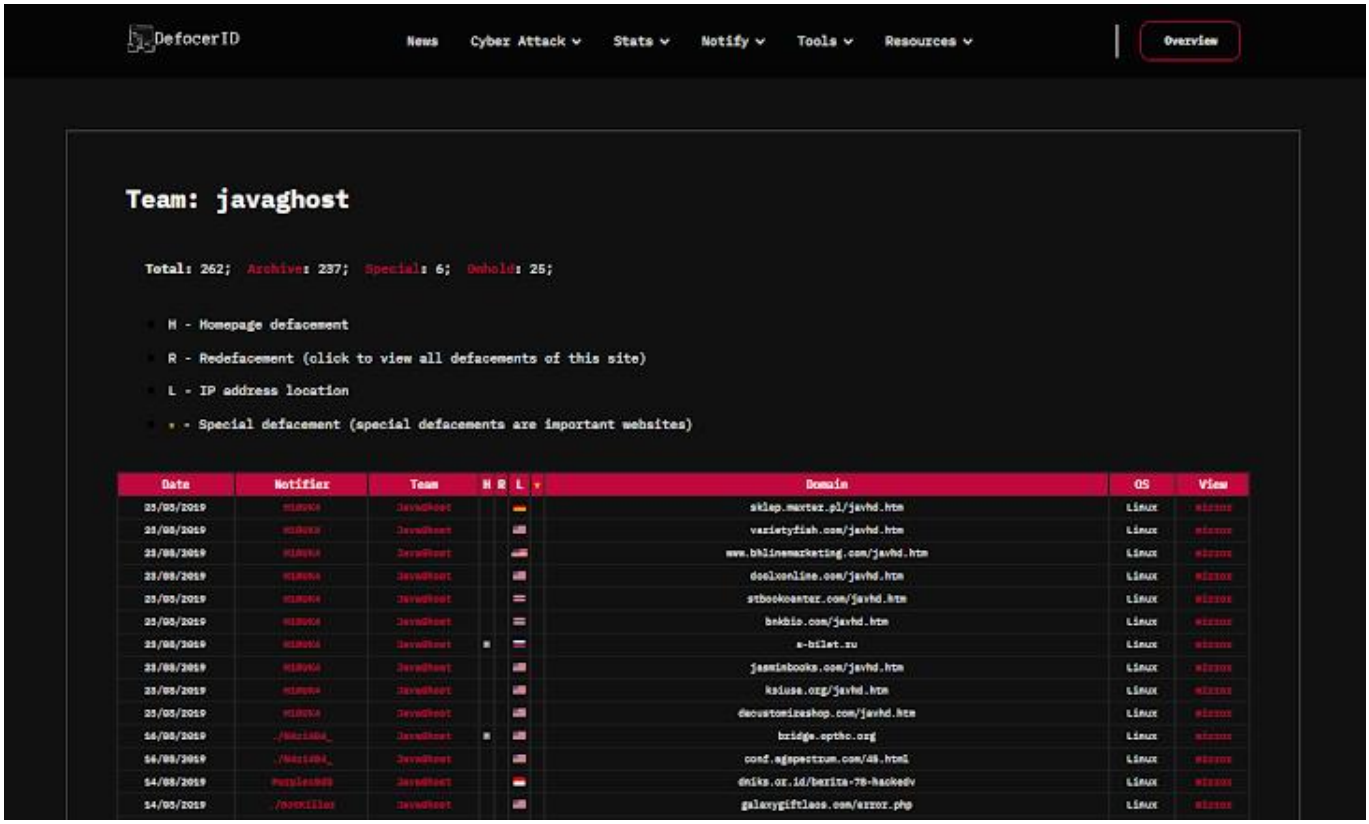
El grupo de ciberseguridad está rastreando esta actividad bajo el nombre TGR-UNK-0011, una amenaza de motivación desconocida que presenta similitudes con el grupo JavaGhost, el cual ha estado activo desde 2019.

 Evolución de la amenaza
Inicialmente, JavaGhost se enfocaba en desfigurar sitios web. Sin embargo, en 2022, el grupo cambió su enfoque para enviar correos electrónicos de phishing con fines financieros, explicó la investigadora de seguridad Margaret Kelley.

 Cómo operan los atacantes
Estos ataques no explotan vulnerabilidades en AWS, sino que se aprovechan de configuraciones incorrectas en los entornos de las víctimas. Específicamente, los atacantes acceden a claves de acceso de AWS expuestas y utilizan servicios como Amazon Simple Email Service (SES) y WorkMail para enviar correos de phishing.

Esta táctica les permite:
 Evitar pagar por infraestructura propia para sus ataques.
 Evadir sistemas de seguridad de correo electrónico, ya que los mensajes provienen de una entidad legítima que las organizaciones ya conocen.

 Acceso inicial y evasión de defensas
JavaGhost obtiene claves de acceso a largo plazo de usuarios de IAM para acceder a entornos de AWS a través de la línea de comandos (CLI). Entre 2022 y 2024, el grupo ha refinado sus técnicas, implementando estrategias avanzadas de evasión para ocultar su identidad en los registros de CloudTrail, una táctica similar a la utilizada por el grupo Scattered Spider.



Una vez dentro de la cuenta AWS de la víctima, los atacantes:
 Generan credenciales temporales y URLs de inicio de sesión para acceder a la consola.
 Usan SES y WorkMail para establecer su infraestructura de phishing, creando nuevos usuarios y credenciales SMTP.
 Crean múltiples usuarios de IAM, algunos activos en los ataques y otros que parecen estar diseñados para garantizar persistencia a largo plazo.
 Configuran roles de IAM con políticas de confianza para acceder a la cuenta desde otra cuenta de AWS bajo su control.

 Firma del ataque
Una de las marcas distintivas de JavaGhost es la creación de grupos de seguridad en EC2 con el nombre «Java_Ghost» y la descripción: «We Are There But Not Visible» («Estamos ahí, pero no somos visibles»).

Estos grupos no tienen reglas de seguridad ni se adjuntan a ningún recurso, pero su presencia queda registrada en los eventos de CreateSecurityGroup en CloudTrail.