Se ha descubierto una reciente herramienta de piratería basada en Python denominada FBot, la cual está dirigida a servidores web, servicios en la nube, sistemas de gestión de contenido (CMS) y plataformas SaaS como Amazon Web Services (AWS), Microsoft 365, PayPal, Sendgrid y Twilio.

> El investigador de seguridad de SentinelOne, Alex Delamotte, compartió en un informe que *«entre las características destacadas se incluyen la extracción de credenciales para ataques de spam, herramientas de secuestro de cuentas de AWS y funciones que permiten ataques contra PayPal y diversas cuentas SaaS».*

FBot se suma a la lista de herramientas de piratería en la nube, como AlienFox, GreenBot (también conocido como Maintance), Legion y Predator, siendo estos cuatro últimos los cuales comparten similitudes a nivel de código con AndroxGh0st.

Según SentinelOne, FBot es *«relacionado pero distinto de estas familias»,* ya que no hace referencia a ningún código fuente de AndroxGh0st, aunque muestra similitudes con Legion, que salió a la luz el año pasado.

El propósito principal de esta herramienta es apoderarse de servicios en la nube, SaaS y web, además de recolectar credenciales para obtener acceso inicial y monetizarlo mediante la venta de dicho acceso a otros actores.

FBot, además de generar claves API para AWS y Sendgrid, incluye diversas funciones como la generación de direcciones IP aleatorias, la ejecución de escáneres de IP inversos e incluso la validación de cuentas de PayPal y las direcciones de correo electrónico asociadas a estas cuentas.

> *«El script inicia la solicitud de la API de Paypal a través del sitio web hxxps://www.robertkalinkin.com/index.php, que es un sitio de ventas minoristas del diseñador de moda lituano Robert Kalinkin. Es interesante observar que todas las*

> *muestras identificadas de FBot utilizan este sitio web para autenticar las solicitudes de la API de Paypal, y varias muestras de Legion Stealer también lo hacen»,* destacó Delamotte.

Además, FBot incorpora características específicas para AWS, como la verificación de detalles de configuración de correo electrónico del AWS Simple Email Service (SES) y la determinación de las cuotas de servicio EC2 de la cuenta objetivo. La funcionalidad relacionada con Twilio se utiliza de manera similar para recopilar detalles sobre la cuenta, como el saldo, la moneda y los números de teléfono asociados a la cuenta.

Las características de esta herramienta no terminan aquí, ya que el malware también tiene la capacidad de extraer credenciales de archivos de entorno de Laravel.

La empresa de ciberseguridad afirma haber descubierto muestras de FBot desde julio de 2022 hasta tan recientemente como este mes, lo que sugiere que se está utilizando activamente en entornos reales. No obstante, en la actualidad no se sabe si la herramienta se mantiene activamente ni cómo se distribuye a otros actores.

> *«Encontramos indicios de que FBot es producto de trabajo de desarrollo privado, por lo que las versiones contemporáneas podrían distribuirse a través de una operación a menor escala»*, señaló Delamotte.

> *«Esto concuerda con la tendencia de que las herramientas de ataque en la nube son 'bots privados' personalizados para el comprador individual, un patrón que es prevalente en las construcciones de AlienFox».*