Esta campaña, identificada con el nombre en clave FreeDrain por las firmas de inteligencia de amenazas SentinelOne y Validin, ha sido diseñada para engañar a los usuarios y obtener acceso a sus carteras digitales.

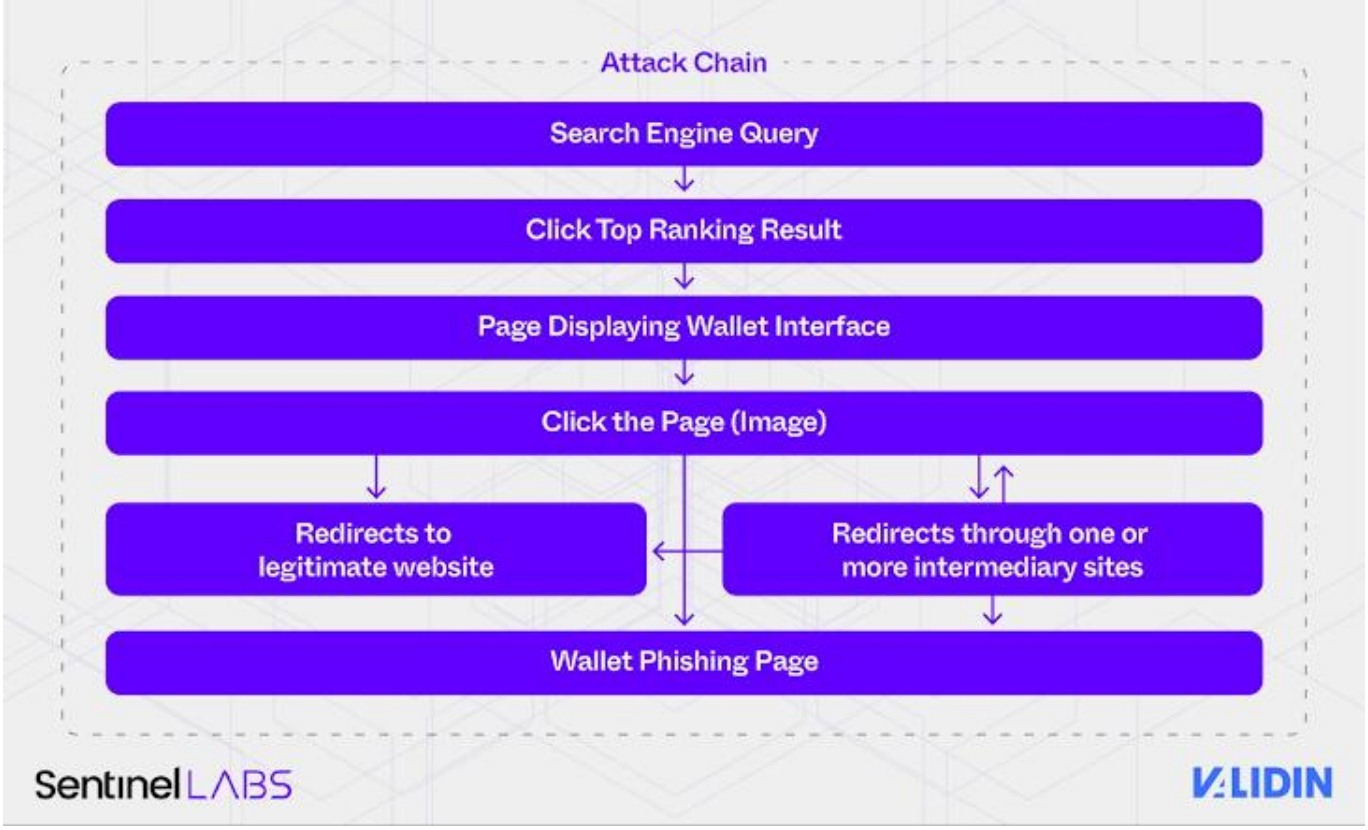
Según los investigadores Kenneth Kinion, Sreekar Madabushi y Tom Hegel, FreeDrain utiliza técnicas de manipulación en motores de búsqueda (SEO), plataformas web gratuitas como GitBook, Webflow y GitHub, así como redirecciones encadenadas para dirigir a los usuarios hacia sitios falsos. Estos sitios simulan ser interfaces legítimas de carteras de criptomonedas, y están diseñados para robar las frases semilla de las víctimas, lo que permite vaciar sus fondos.

Más de 38,000 subdominios únicos han sido detectados como parte de esta red, alojando páginas trampa en infraestructuras como Amazon S3 y Azure Web Apps. Los atacantes operan en horarios de oficina típicos dentro de la zona horaria de la India (IST), según los patrones observados en sus publicaciones en GitHub.

El ataque se activa cuando los usuarios buscan términos como «saldo Trezor wallet» en buscadores como Google o DuckDuckGo, y hacen clic en enlaces maliciosos bien posicionados. Los usuarios son redirigidos a páginas que imitan sitios confiables, donde se les pide ingresar su frase semilla. Una vez que lo hacen, un sistema automatizado roba sus fondos en cuestión de minutos.

Además, se sospecha que los textos utilizados en estas páginas fraudulentas fueron generados con herramientas de inteligencia artificial como GPT-4o de OpenAI, demostrando cómo los actores maliciosos están utilizando IA generativa para crear contenido de forma masiva.

Los operadores de FreeDrain también aumentan la visibilidad de sus páginas al inyectar miles de comentarios basura en sitios web mal gestionados, una técnica conocida como spamdexing, para manipular los resultados de los buscadores.




Algunos aspectos de esta campaña ya habían sido documentados por Netskope Threat Labs desde agosto de 2022. Para octubre de 2024, los atacantes seguían creando sitios falsos que imitaban servicios populares como Coinbase, MetaMask, Phantom, Trezor y Bitbuy.

Los investigadores advierten que el uso de plataformas gratuitas para hospedar contenido malicioso no es nuevo, y que, sin mayores controles, estos servicios seguirán siendo explotados. FreeDrain representa un modelo moderno de phishing a gran escala: difícil de rastrear, fácil de restablecer y resistente a los intentos de eliminación.

En paralelo, Check Point Research ha identificado otra campaña de phishing avanzada que utiliza Discord para atacar a usuarios de criptomonedas, usando una herramienta conocida como Inferno Drainer, ofrecida como servicio (Drainer-as-a-Service).

Esta operación secuestra enlaces de invitación expirados de Discord para atraer víctimas a servidores maliciosos, y emplea el sistema de autenticación OAuth2 de Discord para evitar ser detectados por sistemas automáticos.

Entre septiembre de 2024 y marzo de 2025, se estima que más de 30,000 carteras digitales fueron comprometidas por Inferno Drainer, causando pérdidas por al menos 9 millones de dólares. Aunque el grupo aseguró haber cesado actividades en noviembre de 2023, los expertos encontraron evidencia de que aún sigue activo, utilizando contratos inteligentes de un solo uso y configuraciones cifradas para evitar su detección.

También se ha descubierto una campaña de malvertising (publicidad maliciosa) que usa anuncios en Facebook para hacerse pasar por plataformas de criptocomercio como Binance, Bybit y TradingView. Estas campañas redirigen a los usuarios a sitios engañosos que les piden instalar un cliente de escritorio.

Según Bitdefender, estos sitios analizan si el visitante proviene de un anuncio real o de un entorno automatizado, como una sandbox de análisis. Si detectan un entorno sospechoso, muestran contenido inofensivo para evitar ser descubiertos.

El instalador malicioso muestra una interfaz falsa para recolectar datos o ejecutar comandos ocultos durante horas si sospecha que está siendo monitoreado. Los anuncios fueron promovidos desde cientos de cuentas de Facebook, apuntando principalmente a hombres mayores de 18 años en Bulgaria y Eslovaquia.

Este tipo de campañas muestran un enfoque mixto: combinan el engaño visual en la interfaz con servicios maliciosos ejecutados localmente, y logran mantener operaciones evasivas y resistentes mediante actualizaciones constantes y análisis del entorno de las víctimas.