Un actor de amenazas con motivación económica, identificado bajo el alias *UNC5142*, ha sido observado aprovechando contratos inteligentes en blockchain como método para distribuir troyanos de robo de información, entre ellos *Atomic (AMOS)*, *Lumma*, *Rhadamanthys* (también conocido como *RADTHIEF*) y *Vidar*, con objetivos en sistemas tanto Windows como macOS.

"UNC5142 se distingue por utilizar sitios WordPress comprometidos y una técnica llamada 'EtherHiding', que consiste en ocultar código malicioso o datos dentro de una blockchain pública como la BNB Smart Chain", explicó el *Grupo de Inteligencia de Amenazas de Google (GTIG)* en un informe compartido con Masterhacks.

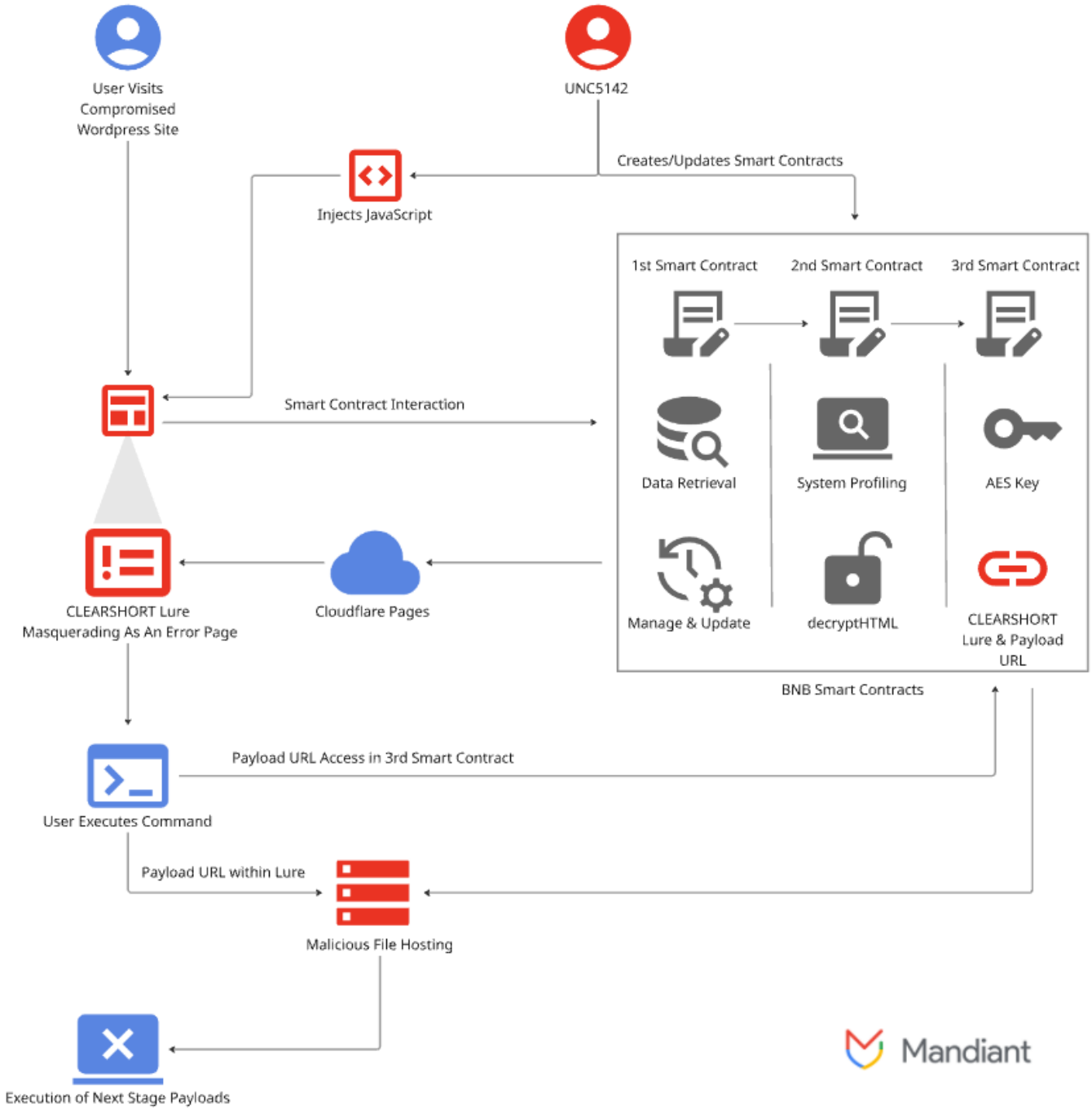
Hasta junio de 2025, Google informó que había detectado alrededor de 14,000 páginas web con código JavaScript inyectado asociado a UNC5142, lo que sugiere un ataque indiscriminado a sitios WordPress vulnerables. No obstante, la compañía tecnológica señaló que no se han detectado nuevas actividades del grupo desde el 23 de julio de 2025, lo que podría indicar una pausa o un cambio en su estrategia operativa.

EtherHiding fue documentado por primera vez por *Guardio Labs* en octubre de 2023, cuando se identificaron ataques que servían código malicioso usando contratos en la Binance Smart Chain (BSC), a través de sitios web infectados que mostraban alertas falsas de actualización del navegador.

Un componente clave en esta cadena de ataque es un descargador JavaScript en varias fases, conocido como *CLEARSHORT*, que facilita la entrega de malware desde los sitios comprometidos. La primera etapa consiste en un script malicioso insertado en los sitios, el cual recupera una segunda etapa interactuando con un contrato inteligente malicioso alojado en la blockchain BNB Smart Chain. Este script inicial suele añadirse a archivos de plugins, temas e incluso directamente en la base de datos de WordPress.

El contrato inteligente tiene la función de obtener una página de destino *CLEARSHORT* desde un servidor externo. Esta página emplea la técnica de ingeniería social conocida como *ClickFix*, diseñada para engañar a los usuarios y hacer que ejecuten comandos maliciosos en

el cuadro de diálogo «Ejecutar» de Windows o en la terminal de macOS, con el fin de instalar el malware tipo stealer en sus dispositivos. Desde diciembre de 2024, estas páginas suelen estar alojadas en dominios .dev protegidos por Cloudflare y se entregan en formato cifrado.



En sistemas Windows, el comando malicioso ejecuta un archivo de Aplicación HTML (HTA)

descargado desde una URL de MediaFire, que luego lanza un script en PowerShell. Este script evade defensas, recupera la carga final cifrada desde GitHub, MediaFire o infraestructura propia del atacante, y ejecuta el malware directamente en la memoria sin escribirlo en disco.

En los ataques dirigidos a macOS en febrero y abril de 2025, los atacantes emplearon señuelos *ClickFix* que incitaban al usuario a ejecutar un comando *bash* en la Terminal, lo cual descargaba un script que, mediante *curl*, obtenía la carga útil del troyano *Atomic Stealer* desde un servidor remoto.

Se ha determinado que *CLEARSHORT* es una variante de *ClearFake*, una estructura JavaScript maliciosa estudiada en profundidad por la firma de ciberseguridad francesa *Sekoia* en marzo de 2025. *ClearFake* se propaga en sitios comprometidos para instalar malware mediante la técnica de *drive-by download*. Se tiene constancia de su actividad desde julio de 2023, y su uso de *ClickFix* comenzó en mayo de 2024.

El uso de blockchain aporta múltiples ventajas, ya que esta técnica innovadora permite camuflarse entre actividades legítimas de Web3 y además incrementa la resistencia de las operaciones de UNC5142 frente a detecciones o intentos de desactivación.

Google señaló que las campañas de este actor han evolucionado significativamente en el último año, pasando de utilizar un único contrato a implementar un sistema más complejo basado en tres contratos inteligentes desde noviembre de 2024, con ajustes adicionales observados a inicios de enero de 2025.

“Esta nueva arquitectura está inspirada en un principio de diseño de software legítimo conocido como patrón proxy, que los desarrolladores emplean para permitir actualizaciones en sus contratos”, explicó la compañía.

“La estructura actúa como una arquitectura eficiente de tipo Router-Logic-Storage, donde cada contrato cumple una función específica. Esto permite realizar cambios rápidos en elementos críticos del ataque, como la URL de la página de destino o la clave de descifrado, sin necesidad de modificar el JavaScript en los sitios web comprometidos. Como resultado,

las campañas se vuelven mucho más dinámicas y difíciles de neutralizar."

UNC5142 logra esto aprovechando la naturaleza modificable de los datos en un contrato inteligente (aunque el código del contrato en sí no puede cambiar una vez desplegado), lo que les permite alterar la URL del malware por un coste de entre $0.25 y $1.50 en tarifas de red por actualización.

Un análisis más detallado reveló que el grupo emplea dos infraestructuras distintas de contratos inteligentes para entregar el malware a través del descargador *CLEARSHORT*. La infraestructura principal fue creada el 24 de noviembre de 2024, mientras que la secundaria fue financiada el 18 de febrero de 2025.

"La infraestructura principal destaca por ser el eje central de la campaña, evidenciado por su fecha temprana de creación y sus actualizaciones constantes," comentó GTIG. *"La infraestructura secundaria parece funcionar como un despliegue paralelo de carácter táctico, probablemente diseñado para respaldar un incremento puntual en la actividad, probar nuevos señuelos o reforzar la resiliencia operativa."*

"Dada la frecuencia de actualizaciones en la cadena de infección, el ritmo sostenido de operaciones, el elevado número de sitios comprometidos y la variedad de cargas maliciosas distribuidas en el último año y medio, es probable que UNC5142 haya obtenido cierto grado de éxito en sus campañas."