Investigadores en ciberseguridad han alertado sobre un incremento en la creación de páginas de phishing mediante una herramienta de creación de sitios web llamada Webflow, ya que los actores maliciosos continúan explotando servicios legítimos como Cloudflare y Microsoft Sway para sus propios fines.

> *«Las campañas buscan capturar información confidencial de diversas billeteras de criptomonedas, incluyendo Coinbase, MetaMask, Phantom, Trezor y Bitbuy, así como credenciales de inicio de sesión para múltiples plataformas de correo web empresarial y de Microsoft 365»*, indicó Jan Michael Alcantara, investigador de Netskope Threat Labs, en un análisis.

La empresa de ciberseguridad reportó un aumento de diez veces en el tráfico hacia las páginas de phishing diseñadas con Webflow entre abril y septiembre de 2024, con ataques dirigidos a más de 120 organizaciones a nivel mundial. La mayoría de los objetivos se encuentran en América del Norte y Asia, cubriendo sectores como los servicios financieros, banca y tecnología.

Se ha observado que los atacantes utilizan Webflow para crear páginas de phishing independientes, además de redirigir a los usuarios desprevenidos a otras páginas de phishing bajo su control.

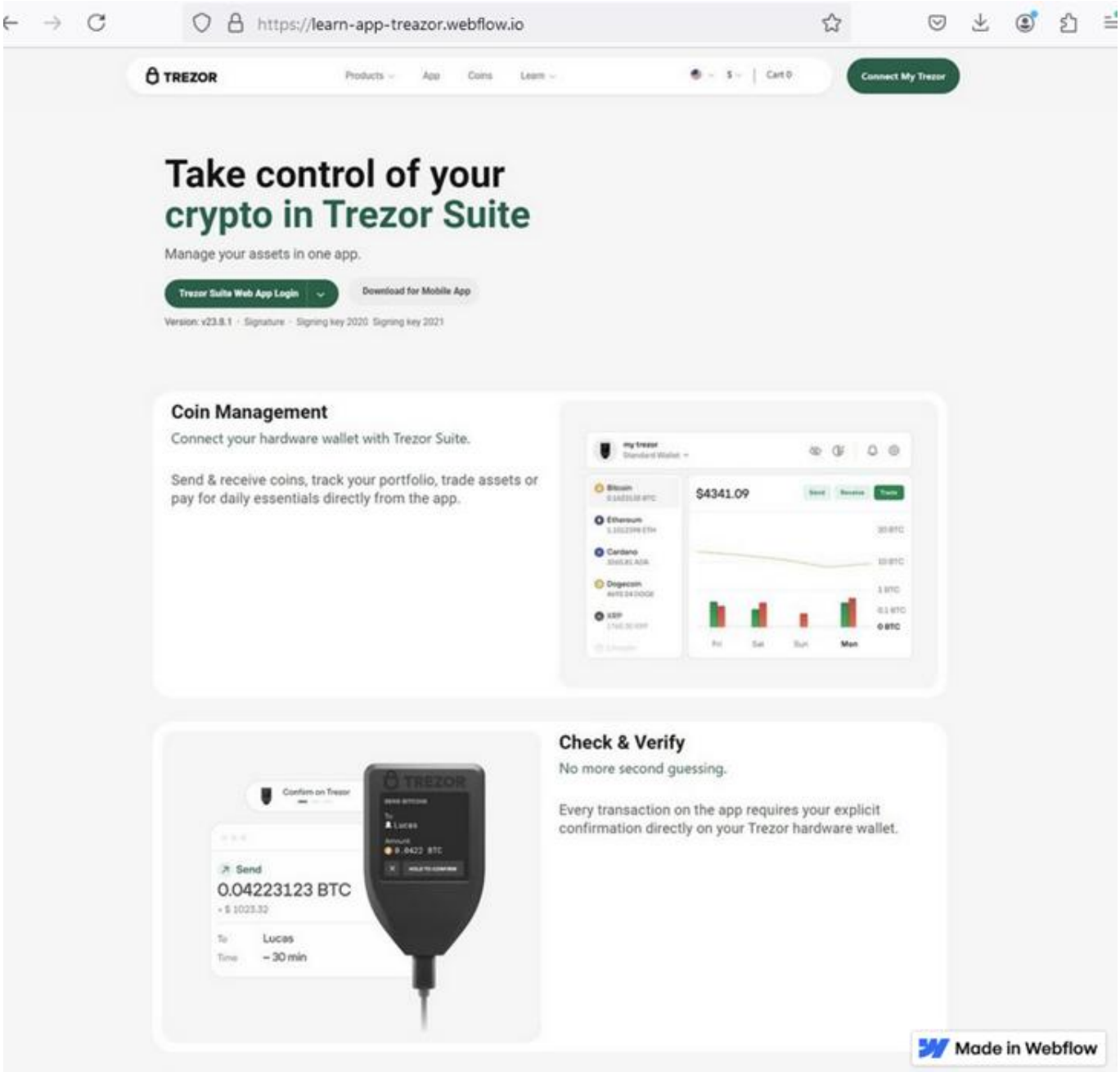
> *«La primera opción proporciona a los atacantes discreción y facilidad, ya que no necesitan escribir o detectar código de phishing, mientras que la segunda permite al atacante realizar acciones más complejas cuando sea necesario»*, explicó Michael Alcantara.

Lo que hace que Webflow sea más atractivo que Cloudflare R2 o Microsoft Sway es que permite a los usuarios crear subdominios personalizados sin costo adicional, a diferencia de los subdominios alfanuméricos generados automáticamente que suelen levantar sospechas:

- Cloudflare R2: `https://pub-<32_caracteres_alfanuméricos>.r2.dev/pagina.htm`
- Microsoft Sway: `https://sway.cloud.microsoft/{16_caracteres_alfanuméricos}?ref={opcion_de_compartir}`

Para aumentar la efectividad del ataque, las páginas de phishing imitan cuidadosamente las páginas de inicio de sesión legítimas para engañar a los usuarios a ingresar sus credenciales, las cuales, en algunos casos, son extraídas a otro servidor.

Netskope también detectó sitios de estafa de criptomonedas en Webflow que muestran una captura de pantalla de la página de inicio legítima de una billetera como su página falsa de aterrizaje y redirigen al visitante al sitio de estafa real al hacer clic en cualquier parte de la página.



El objetivo final de la campaña de phishing en criptomonedas es obtener las frases de recuperación de las víctimas, lo que permite a los atacantes tomar control de las carteras y drenar los fondos.

En los ataques identificados por la empresa de ciberseguridad, a los usuarios que ingresan la frase de recuperación se les muestra un mensaje de error que indica que su cuenta ha sido suspendida por *«actividad no autorizada y fallo de identificación».* El mensaje también insta al usuario a contactar al equipo de soporte iniciando un chat en línea en Tawk.to.

Es importante señalar que servicios de chat como LiveChat, Tawk.to y Smartsupp han sido utilizados indebidamente en una campaña de estafa de criptomonedas llamada CryptoCore, según Avast.

> *«Los usuarios deben acceder a páginas importantes, como su portal bancario o correo electrónico, ingresando la URL directamente en el navegador en lugar de utilizar motores de búsqueda o hacer clic en enlaces externos»,* recomendó Michael Alcantara.

Este desarrollo se produce al mismo tiempo que cibercriminales promueven en la dark web nuevos servicios anti-bot que afirman poder eludir las advertencias de navegación segura de Google en Chrome.

> *«Los servicios anti-bot, como Otus Anti-Bot, Remove Red y Limitless Anti-Bot, se han vuelto una pieza clave en las operaciones de phishing complejas. Estos servicios buscan impedir que los rastreadores de seguridad identifiquen y bloqueen las páginas de phishing»,* señaló SlashNext en un informe reciente.
>
> *«Al filtrar bots de seguridad y disfrazar las páginas de phishing de los escáneres, estas herramientas aumentan la duración de los sitios maliciosos, ayudando a los delincuentes a evadir la detección por más tiempo».*

También se han descubierto campañas activas de malspam y malvertising que están

propagando un malware en evolución llamado WARMCOOKIE (también conocido como BadSpace), que sirve como canal para otros malwares como CSharp-Streamer-RAT y Cobalt Strike.

> *«WARMCOOKIE ofrece una variedad de funcionalidades útiles para los atacantes, incluyendo despliegue de cargas, manipulación de archivos, ejecución de comandos, captura de pantallas y persistencia, lo que lo hace atractivo para su uso en sistemas comprometidos, facilitando el acceso persistente a largo plazo dentro de redes afectadas»*, explicó Cisco Talos.

Un análisis del código fuente sugiere que el malware probablemente fue desarrollado por los mismos actores que Resident, un implante post-compromiso desplegado como parte de un conjunto de intrusión llamado TA866 (también conocido como Asylum Ambuscade), junto con el ladrón de información Rhadamanthys. Estas campañas han apuntado principalmente al sector manufacturero, seguido de cerca por el gobierno y servicios financieros.

> *«Aunque el objetivo a largo plazo de las campañas de distribución parece indiscriminado, la mayoría de los casos donde se han observado cargas adicionales ocurrieron en Estados Unidos, con casos adicionales en Canadá, Reino Unido, Alemania, Italia, Austria y Países Bajos»*, señaló Talos.