Los operadores detrás de la plataforma de phishing como servicio (PhaaS) Darcula están preparando una nueva versión que permitirá a ciberdelincuentes y clientes potenciales duplicar cualquier sitio web legítimo de una marca y transformarlo en una página fraudulenta. Esto reduce aún más la necesidad de conocimientos técnicos para llevar a cabo ataques de phishing a gran escala.

La versión más reciente de esta suite de phishing *«marca un cambio importante en las capacidades delictivas, disminuyendo la barrera de entrada para que los atacantes apunten a cualquier marca con campañas de phishing sofisticadas y personalizables»*, explicó Netcraft en un nuevo informe.

La empresa de ciberseguridad ha identificado y bloqueado más de 95,000 dominios de phishing asociados con Darcula, cerca de 31,000 direcciones IP, y ha desmantelado más de 20,000 sitios fraudulentos desde su primera detección a finales de marzo de 2024.

El cambio más notable en Darcula es la introducción de una función que permite a cualquier usuario generar de inmediato un kit de phishing para cualquier marca.

«La versión mejorada y actualizada ya está disponible para pruebas», anunciaron los desarrolladores del servicio en un mensaje publicado el 19 de enero de 2025 en un canal de Telegram con más de 1,200 seguidores.

> *«Ahora puedes modificar el front-end por tu cuenta. Con darcula-suite, puedes crear un front-end en solo 10 minutos».*

Para ello, el usuario solo necesita ingresar la URL del sitio web de la marca que desea imitar en una interfaz web. La plataforma, mediante herramientas de automatización como Puppeteer, captura el código HTML y todos los recursos necesarios.

Posteriormente, el usuario puede seleccionar los elementos HTML que desea modificar e insertar el contenido malicioso, como formularios de pago o credenciales de inicio de sesión,

para que coincida visualmente con la página legítima. Una vez completado, la página de phishing es cargada en un panel de administración.

> *«Al igual que otros servicios de software como servicio, la plataforma PhaaS darcula-suite proporciona paneles de administración que facilitan a los estafadores la gestión de sus campañas»,* señaló el investigador en ciberseguridad Harry Freeborough.
>
> *«Después de ser creados, estos kits se suben a otra plataforma donde los atacantes pueden administrar sus campañas activas, revisar los datos recopilados y supervisar sus operaciones fraudulentas».*

Además de ofrecer paneles de control con métricas detalladas sobre el rendimiento de las campañas de phishing, Darcula v3 introduce una funcionalidad adicional que permite convertir los datos de tarjetas de crédito robadas en imágenes digitales de las tarjetas, listas para ser escaneadas y agregadas a billeteras digitales con fines ilícitos. Estas tarjetas virtuales se cargan en dispositivos desechables y luego se venden a otros delincuentes.

Actualmente, la herramienta sigue en fase de pruebas internas. En un mensaje posterior, publicado el 10 de febrero de 2025, el creador del malware declaró: *«He estado ocupado últimamente, así que la actualización de la versión 3 se retrasará unos días».*