Recientes investigaciones han desvelado que agentes de amenaza están utilizando los Túneles de Cloudflare de manera abusiva para establecer canales de comunicación encubiertos desde sistemas comprometidos y mantener un acceso persistente.

> *«Cloudflared posee una funcionalidad muy similar a ngrok. No obstante, se diferencia de ngrok en el sentido de que proporciona muchas más capacidades de forma gratuita, incluyendo la habilidad de gestionar conectividad TCP a través de cloudflared»,* afirmó Nic Finn, un analista sénior de inteligencia de amenazas en GuidePoint Security.

Cloudflared, una herramienta de línea de comandos para los Túneles de Cloudflare, permite a los usuarios crear conexiones seguras entre un servidor web de origen y el centro de datos más cercano de Cloudflare. Esto tiene como fin ocultar las direcciones IP del servidor web, al igual que bloquear ataques de denegación de servicio distribuido (DDoS) de gran volumen y ataques de inicio de sesión por fuerza bruta.

Para un agente de amenaza con un acceso ampliado en un sistema infectado, esta característica ofrece un enfoque prometedor para establecer una posición firme mediante la generación de un token necesario para establecer el túnel desde la máquina afectada.

> *«El túnel se actualiza en cuanto se realiza un cambio en la configuración en el Panel de Control de Cloudflare, lo que permite a los agentes de amenaza activar la funcionalidad solo cuando deseen llevar a cabo actividades en la máquina afectada y luego desactivarla para evitar exponer su infraestructura»,* detalló Finn.

> *«Por ejemplo, el agente de amenazas podría activar la conectividad RDP, recabar información de la máquina víctima y luego desactivar RDP hasta el día siguiente, disminuyendo así las posibilidades de detección o la capacidad de observar el*

> *dominio utilizado para establecer la conexión.»*

De manera aún más inquietante, el adversario podría aprovechar la funcionalidad de Redes Privadas del túnel para acceder sigilosamente a un rango de direcciones IP (es decir, puntos finales dentro de una red local) como si estuvieran *«físicamente ubicados junto a la máquina víctima que aloja el túnel».*

Dicho esto, la técnica ya ha encontrado adeptos en la vida real. A principios de este año, Phylum y Kroll detallaron dos ataques diferentes a la cadena de suministro de software dirigidos al repositorio Python Package Index (PyPI), en los cuales se observó que paquetes fraudulentos descargaban cloudflared para acceder de forma remota al punto final a través de una aplicación web Flask.

> *«Las organizaciones que utilizan los servicios de Cloudflare de manera legítima podrían restringir sus servicios a centros de datos específicos y generar alertas por tráfico de túneles Cloudflared que se dirijan a cualquier lugar excepto a sus centros de datos designados. Este enfoque podría contribuir a detectar túneles no autorizados»,* explicó Finn.

Para identificar posibles usos indebidos de cloudflared, se recomienda que las organizaciones implementen mecanismos de registro adecuados para supervisar comandos inusuales, consultas DNS y conexiones salientes, además de bloquear intentos de descargar el archivo ejecutable.