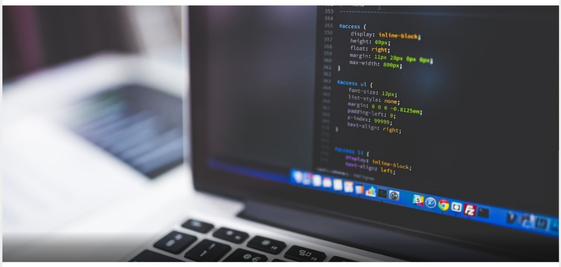
cultura y sociedad

La cara y la cruz de TOR: lucha contra el cibercrimen en la red anónima



Por Lara Muga
Publicado el 31 de mayo de 2025 a las 17:04

El resumen de la noticia

«La red TOR no es el infierno digital que muchos imaginan. Pero sí puede albergarlo». Con esta frase, el investigador de UNIR Facundo Gallo resume la paradoja de una de las tecnologías más controvertidas de nuestro tiempo: una red diseñada para proteger la privacidad, que también puede ser usada como escudo para el crimen.

Y es precisamente en esa fina línea Gallo y su equipo han encontrado una forma novedosa de actuar: una metodología de monitorización que permite anticipar y detectar ciberataques y delitos digitales sin vulnerar la privacidad de los usuarios legítimos.

Este trabajo ha sido desarrollado por investigadores de UNIR y la Universidad de Granada, y ha puesto el foco en los llamados nodos de salida de la red TOR, un punto estratégico desde el cual se puede observar una parte del tráfico que abandona esta red anónima. Lo que sorprende en este estudio es que solo un 7,8 por ciento de ese tráfico tiene relación con actividades maliciosas.

Gallo describe TOR como una red de sistemas informáticos capaz de establecer una comunicación cifrada y anónima entre los usuarios y los denominados servicios ocultos, que básicamente son páginas web inaccesibles desde Google u otro tipo de buscador al uso. Por lo tanto, la red TOR es parte constituyente de lo que conocemos como Deep Web o internet profunda, ya que contiene un conjunto de servicios que requiere de mecanismos adicionales para ser visualizados.

Para muchos, «es la herramienta para escapar de la censura, proteger datos sensibles o comunicarse libremente en países donde hablar con libertad puede costar caro. Para otros, es la puerta a la dark web, el "lado oscuro" de internet donde se comercializan drogas, armas, datos robados o pornografía infantil». Además, donde se alojan innumerables páginas web con servicios de sicarios, venta de estupefacientes, tráficos de órganos, y material relacionado con abuso sexual infantil.

Según Gallo, "la mayor parte de las búsquedas en TOR son lícitas. Se accede a redes sociales, a buscadores, a contenidos de telefonía o noticias. Pero, efectivamente, existe un uso criminal de esta red, y nuestra labor es anticiparnos a ello."

Una labor que no invade sistemas ni intercepta información privada. «Nosotros no somos policías, somos investigadores. No accedemos a datos personales ni comprometemos derechos fundamentales». Entonces, ¿cómo lo hacen? Instalando un nodo de salida dentro de la red TOR, es decir, el último servidor por donde pasa una conexión antes de llegar al sitio web de destino.

Este nodo actúa como una ventana desde la que pueden observar qué tipo de peticiones hacen los usuarios, especialmente cuando visitan páginas normales (de la llamada surface web). «Es como colocar una radio en lo alto de una montaña e intentar escuchar las conversaciones no cifradas del aeropuerto más cercano», compara Gallo.

Prevenir ataques antes de que ocurran

El verdadero valor de esta técnica radica en su capacidad preventiva. Monitorizando el tráfico saliente, los investigadores pueden detectar en tiempo real intentos de ciberataques dirigidos a infraestructuras críticas: hospitales, plantas eléctricas, estaciones de tratamiento de agua.... «Hace no mucho, una persona accedió a una depuradora en Estados Unidos e intentó alterar los niveles químicos del agua para envenenar a la población. Con técnicas como la nuestra, ese tipo de ataques pueden bloquearse antes de que lleguen a materializarse».

Además, este tipo de monitoreo puede ayudar a identificar servicios activos en el mercado negro, contribuyendo a que las fuerzas del orden puedan actuar más eficazmente. Pero, como toda tecnología, puede ser usada con fines oscuros. «Nuestro objetivo no es criminalizar a TOR, sino mostrar que es posible detectar amenazas sin violar derechos».

Pese a que el 90 por ciento del tráfico monitorizado en este estudio era legítimo, eso no significa que la red esté libre de riesgos. En investigaciones anteriores, el equipo de Gallo llegó a contabilizar más de 30 millones de enlaces activos dedicados a la pornografía infantil solo dentro de la red TOR. «Cada vez que repito esa cifra, se me hiela la sangre», confiesa.

En esos casos, aplican otras estrategias, como la creación de señuelos, diseñados para rastrear comportamientos delictivos y geo-posicionar a los responsables. Cuando eso ocurre, la información es inmediatamente derivada a la Guardia Civil, con la que mantienen un canal directo de colaboración. «Nosotros no podemos detener a nadie, pero nuestro trabajo puede ser útil para quienes sí pueden hacerlo».

Más allá del impacto académico, esta investigación abre la puerta a nuevas líneas de trabajo en el campo de la ciberseguridad, la inteligencia artificial aplicada al crimen digital y la ética tecnológica. «Demostramos que es posible construir herramientas que equilibren protección y privacidad ayudando a prevenir sin vulnerar».

Y, sobre todo, Gallo recuerda que el conocimiento no es una trinchera, sino un puente. «Todos hemos oído hablar de la deep web como un pozo de horrores. Pero hay que mirar más allá del mito. La mayoría de las veces, los usuarios solo buscan protegerse. Nuestra labor está en distinguir lo legítimo de lo delictivo y dar herramientas para hacerlo»

Más: UNIR

recomendado para ti


Mohamed Ali


La biblioteca Rafael Azcona está que arde


Un banco al más puro estilo Michael Jackson 'baila' en la calle Beratúa

El tiempo para este domingo, 1 de junio, en La Rioja

última hora


TINTA Y TINTO
Mohamed Ali


EL SERENO
La biblioteca Rafael Azcona está que arde


EL SERENO
Un banco al más puro estilo Michael Jackson 'baila' en la calle Beratúa