NOTA DE PRENSA

Una nueva metodología de monitorización para luchar contra el cibercrimen en la red anónima TOR

- **Investigadores de la Universidad Internacional de La Rioja (UNIR) y la Universidad de Granada proponen una novedosa técnica, basada en la implementación de nodos de salida del tráfico, que agiliza la detección precoz de ciberataques dirigidos a objetivos críticos y la identificación de mercados ilícitos (armas, droga, etc.).**

- **Los hallazgos revelan que solo un 7,8% del tráfico se asocia con sitios de reputación maliciosa (vinculados a la distribución de malware, ataques de phishing, discursos de odio, terrorismo, violencia, etc.), contradiciendo la imagen de TOR como una red eminentemente delictiva.**

Logroño/Madrid, 12 de mayo de 2025.-

La monitorización de los nodos de salida emerge como una estrategia prometedora para fortalecer la prevención del crimen en la red anónima TOR. Esta técnica posibilita una comprensión profunda del tráfico que transita por esta infraestructura digital y permite anticipar y contrarrestar su uso con fines delictivos.

Investigadores de la **Universidad Internacional de La Rioja** (UNIR) y la **Universidad de Granada** han validado esta propuesta en un estudio revelador.

Sus hallazgos indican que solo un 7,8% del tráfico analizado se asocia con sitios de reputación maliciosa (vinculados a la distribución de malware, ataques de phishing, discursos de odio, terrorismo, violencia, etc.).

Este dato contradice la visión predominante de la red TOR como un espacio eminentemente ilícito, ya que la mayor parte del tráfico saliente (casi el 90%) se dirige a sitios web legítimos, incluyendo empresas, redes sociales y buscadores.

La metodología empleada en esta investigación tiene potencial para la detección temprana de ciberataques dirigidos a objetivos críticos y en la identificación proactiva de mercados ilícitos que operan en la Dark Web, lo que supone un avance en la lucha contra el cibercrimen.

Basada en la monitorización de nodos de salida, posibilita la observación del tráfico no cifrado en el momento en que abandona la red TOR.

Los nodos de salida son los últimos servidores a los que llega una información tras un proceso de rebote de información entre múltiples nodos, que hace muy difícil rastrear el origen de la comunicación. Es el servidor que finalmente envía la información al sitio web o servicio al que se está tratando acceder. Su monitorización ayuda a prevenir actividades ilegales, porque es el punto donde la información se vuelve visible antes de llegar a su destino.

Para llevar a cabo el estudio, los investigadores analizaron el flujo de datos que emergía hacia la internet convencional, centrándose en las peticiones que los usuarios de TOR realizaban a sitios de la Surface Web.

Con este fin, desplegaron estratégicamente un nodo de salida dentro de la red, que actuó como una "ventana" de observación. A través de este nodo, monitorizaron y registraron las solicitudes de nombres de dominio (DNS), las "direcciones" de internet, que los usuarios de TOR intentaban visitar. Tras un exhaustivo procesamiento y análisis de miles de estas peticiones, los resultados fueron concluyentes: la vasta mayoría de los destinos correspondían a sitios web de uso cotidiano.

Agiliza la detección precoz

"La metodología propuesta despliega su potencial preventivo en dos vertientes fundamentales. En primer lugar, la implementación de nodos de salida en la red TOR agiliza la detección precoz de tráfico malicioso –y potenciales ciberataques– dirigidos a infraestructuras estratégicas y esenciales, como centrales eléctricas o plantas de tratamiento de agua. En segundo lugar, facilita la identificación de servicios activos en el mercado negro de internet –venta de estupefacientes, tráfico de armas, etc.–, lo que, en última instancia, contribuye a reducir la superficie de exposición ante ciberamenazas", explica **Facundo Gallo Serpillo**, investigador de UNIR y coautor del estudio junto a **Patricia Saldaña Taboada**.

Los investigadores hacen hincapié en que, aunque el anonimato proporcionado por TOR puede ser explotado para actividades ilícitas, no obstante, su utilidad para la gran mayoría de usuarios, según lo observado en este estudio, radica en la protección de la privacidad.

TOR y la protección de la privacidad

La capacidad de monitorizar el tráfico saliente introduce una nueva dimensión en la seguridad de la red, lo que constituye una herramienta para la prevención del crimen que no menoscaba el derecho a la privacidad de los usuarios legítimos.

El estudio resalta la importancia de comprender el uso legítimo de TOR para la protección de la privacidad en un contexto de creciente preocupación por la vigilancia online y abre nuevas vías para investigar los patrones de uso legítimo de redes de anonimato y para desarrollar estrategias más equilibradas para la seguridad online.

"Debemos reconocer el valor del esfuerzo de los contribuyentes de la red TOR para facilitar el acceso libre a la información y al conocimiento desde la privacidad que ofrece su diseño. Sin embargo, la capacidad de monitorizar el tráfico de salida nos brinda una herramienta útil para fortalecer la seguridad y prevenir actividades ilícitas", añade Gallo.

Este investigador de UNIR desarrolló, en base a un estudio previo, una metodología capaz de geo-posicionar a los usuarios relacionados con el consumo de pornografía infantil en la red TOR a través del despliegue de servicios señuelos (honeypots) dentro del mercado negro.

"En el presente estudio, la inspección del tráfico no cifrado desde un servidor en la capa de salida de TOR nos ofrece una perspectiva radicalmente nueva sobre la seguridad de la red, abriendo caminos concretos para la prevención del cibercrimen", concluye Gallo.

Dos vías para la prevención del cibercrimen

La metodología de monitorización de nodos de salida abre fundamentalmente dos importantes vías para la prevención del cibercrimen:

-Detección temprana de ciberataques: La implementación de nodos de salida para el monitoreo activo facilita la identificación precoz de tráfico malicioso dirigido a infraestructuras críticas y objetivos estratégicos, permitiendo una respuesta proactiva para neutralizar potenciales ciberataques antes de que se materialicen.

-Identificación de mercados ilícitos: Esta metodología permite detectar servicios activos en el mercado negro de internet (venta de drogas, armas, etc.), lo que puede contribuir significativamente a reducir la superficie de exposición ante ciberamenazas y facilitar la labor de las fuerzas del orden en la desarticulación de estas plataformas ilegales.

Las conclusiones de este estudio no solo desmitifican la visión simplista de TOR, sino que también marcan el inicio de nuevas líneas de investigación enfocadas en optimizar la prevención del cibercrimen a través de una comprensión más profunda de los patrones de uso de las redes de anonimato.

Referencias bibliográficas:

Gallo-Serpillo, F., Saldaña-Taboada, P., (2025). In search of light: detecting cybercrime through the analysis of unencrypted traffic on the TOR network. *Information & Communications Technology Law*. https://doi.org/10.1080/13600834.2025.2463715

Gallo-Serpillo, F., J., (2024). Analysis of CSEM offenders on the dark web using honeypots to geolocate IP addresses from Spain. *Computers in Human Behavior*. https://doi.org/10.1016/j.chb.2024.108137

SOBRE UNIR:

UNIR es una universidad que ofrece una educación superior de calidad a través de las tecnologías más innovadoras, siempre con el estudiante en el centro de su actividad. En España, imparte 55 grados, 155 másteres oficiales, 83 títulos propios y 4 programas de doctorado que tienen como objetivo acercar una educación integral y personalizada a los más de 90.000 estudiantes que trabajan en sus aulas presenciales-virtuales desde un centenar de naciones, principalmente en España e Hispanoamérica. Su método de enseñanza, adecuado a las demandas del mercado laboral, hace de UNIR una auténtica palanca social que rompe barreras y ayuda a que cada uno, esté donde esté, cumpla sus sueños de formación y de

progreso personal y profesional. UNIR pertenece al grupo educativo Proeduca, que, junto a otros centros de enseñanza superior y no reglada, atiende a más de 105.000 estudiantes.

PARA MÁS INFORMACIÓN

Departamento de Comunicación UNIR comunicacion@unir.net www.unir.net
Sala de prensa: http://www.unir.net/sala-de-prensa/ Twitter: @UNIRUniversidad y @PrensaUNIR

Paloma Gamarra (La Rioja) 94 121 02 11 ext. 1285 paloma.gamarra@unir.net
Sara Puerto 648 573 733 sara.puerto@unir.net
Isabel Álvarez 639 117 638 isabel.alvarezcastro@unir.net
Diego Caldentey (LATAM) 659 641 848 diego.caldentey@unir.net
José María Fillol (LATAM) 628 902 302 josemaria.fillol@unir.net
Bosco Martín (Director) bosco.martin@unir.net