

Los ciberdelincuentes se pasan de la Dark Web a la encriptación de la Invisible Net

Muchos ciberdelincuentes están ‘migrando’ desde los mercados ilegales de la Dark Web, donde se puede comprar prácticamente cualquier cosa, a la Invisible Net. Se trata de foros encriptados a los que solo se puede acceder por medio de una invitación personal. Esto supone un problema regulatorio, pues dificulta el trabajo de la Policía para investigar la Invisible Net

Algunos hackers se están sirviendo de las potentes medidas de ciberseguridad que ofrecen muchas apps de mensajería instantánea para crear la ‘Invisible Net’: una red paralela a Internet creada por grupos organizados de hackers, con el fin de evitar a la Policía en sus turbios negocios ilegales, que hasta ahora se hacían en la la Dark Web.

Según detalla Panda Security en un comunicado de prensa, hay que tener en cuenta que la Invisible Net no es un espacio en sí mismo como la Dark Web, a la que se accede normalmente desde un navegador TOR. La ‘red invisible’ solo existe en los dispositivos de los usuarios que la utilizan, ya sea desde apps encriptadas, grupos de chat a los que solo se accede con invitación, o foros cerrados.

Rastrear la Invisible Net, un problema legal para la Policía

Aunque los ciberdelincuentes organizados suelen conocerse en ‘marketplaces’ de la Dark Web ya no se sienten ‘seguros’ en este tipo de entornos. Esto es porque la Policía consigue tirar de algunos hilos con los que rastrear sus pasos. De este modo, los equipos de hackers que ya se conocen después de haber realizado algún ‘trabajo’, abandonan la Dark Web para comunicarse y compartir documentos por medio de la Invisible Net.

El hecho de que la información que se transmite por medio de este tipo de apps supone un dilema legal, ya que en teoría, las comunicaciones encriptadas solo pueden ser descifradas de extremo a extremo. Es decir, con la regulación actual, sería ilegal interceptar comunicaciones privadas aunque haya la sospecha de que se esté haciendo algo ilegal por medio de las apps de la Invisible Net.

“Al fin y al cabo, la tecnología no es buena o mala, es simplemente algo que mejora un proceso. Lo que sí puede ser bueno o malo es el uso que se haga de ella. El hecho de que nadie pueda espiar lo que comunicamos con nuestros amigos a través de whatsapp es bueno, porque así evitamos miradas indiscretas que podrían viralizar algo personal o incluso robarnos”, destaca Hervé Lambert, Global Consumer Operations Manager de Panda Security.

Sin embargo, la encriptación de extremo a extremo que dan las apps de mensajería instantánea también puede aprovecharse para vender drogas o comerciar con sexo infantil sin que las Fuerzas de Seguridad del Estado puedan rastrearlo. El culpable no es el desarrollador de la tecnología, sino el usuario. Por ello, “es importante que las empresas que desarrollamos software y hardware trabajemos siempre alienadas para que la seguridad de nuestros dispositivos y aplicaciones atienda a un único fin:

la tecnología responsable”, advierte el directivo de Panda Security.

Datos de contacto:

lununcan
667574131

Nota de prensa publicada en: [Madrid](#)

Categorías: [Nacional Internet General Seguridad](#)

NotasdePrensa

<http://www.notasdeprensa.es>