Cómo la dark web está invadiendo a las redes sociales

Hace algunos años, los servicios ilícitos y el contrabando en línea se originaba de manera oculta e imposibles de rastrear de Internet: la dark web.

Las personas que frecuentaban sitios de la dark web sabían cómo aprovechar el anonimato que se ofrece y, a menudo, lograban evadir las fuerzas de seguridad. Sin embargo, después de un rápido avance que ha tenido en los últimos años, este modelo está cambiando.

ESET, compañía especializada en detección proactiva de amenazas, analiza cómo se promocionan productos y servicios ilegales sin reservas en las redes sociales, donde los mercados ilegales están abiertos a la comunidad, a menudo dejando a las fuerzas de seguridad sin mucho margen más que vigilar.

Los constantes cierres de sitios anónimos o de muy bajo perfil, como Silk Road y AlphaBay, y la dificultad para atraer grandes volúmenes de clientes a la dark web han significado que las organizaciones criminales hayan tenido que buscar alternativas para llegar a sus mercados.

Al mismo tiempo, la pandemia de la Covid-19 ayudó a abrir nuevas vías para la actividad delictiva, desde el teletrabajo y todos los riesgos de seguridad que eso implica, pasando por el acceso restringido a los lugares y el uso de pasaportes sanitarios. Las personas se acostumbraron a estar más tiempo que nunca en línea, aumentando las posibilidades de estar en contacto con ofertas ilícitas.

En los últimos años surgieron nuevas plataformas que los delincuentes han cooptado, siendo quizás Telegram el ejemplo más notable.

Telegram es una plataforma completamente legitima de mensajería instantánea gratuita, de código abierto y basada en la nube, que ganó una gran popularidad al ofrecer mensajes y llamadas cifrados de extremo a extremo para que los ISP y otros terceros no puedan acceder a los datos.

La plataforma atrajo la atención de delincuentes que aprovechan estas opciones de privacidad. Se ofrece todo, desde drogas,

dinero falso, detalles de tarjetas de crédito robadas y otros datos personales, hasta servicios de sicarios (o, más bien, estafas de sicarios). En particular, algunos vendedores también están ofreciendo falsos certificados de vacunación contra la Covid-19 o certificados para permitir viajes, cada uno por alrededor de 260 dólares.

“Preocupantemente, estos grupos de Telegram se pueden encontrar en cuestión de minutos y con solo unos pocos clics. Lo que quizás sea aún más desconcertante es la cantidad de usuarios a los que llega esta información, ya que algunos grupos tienen cientos de miles de miembros, abriendo el nuevo mercado ilegal a una gran audiencia. Sin embargo, esto no sucede solamente en Telegram. Usuarios de TikTok también han ofrecido drogas abiertamente. Las drogas clase A pueden encontrarse en estos sitios en segundos, con la facilidad que implica la posibilidad de usar el chat para pedir lo que busca”, comenta Camilo Gutiérrez Amaya, Jefe del Laboratorio de Investigación de ESET Latinoamérica.

Lo que destacan, desde el equipo e investigación de ESET, es cómo operan estas estafas a escala global. Si se compara con la dark web, comprar a través de redes sociales podría parecer menos peligroso, o incluso legal, y eso esto en ESET lo destacan como parte del problema.

“Una apariencia de respetabilidad puede alentar tanto a los vendedores como a los compradores, lo que provoca un aumento de la actividad ilícita. Desafortunadamente, estas ventas a menudo financian más delitos y el ciclo continúa”, agrega Gutiérrez Amaya de ESET.

Los cibercriminales están utilizando la protección de la privacidad subyacente en Telegram y otros servicios. Junto con el uso de redes privadas virtuales (VPN) y otras herramientas para evadir la captura, es difícil rastrear a aquellos que usan Telegram con fines maliciosos. Incluso si los dispositivos fueran incautados (y, de vez en cuando, las grandes operaciones logran esto), es poco probable que haya suficiente o alguna evidencia sólida en los dispositivos debido a la posibilidad de configurar que los mensajes que desaparecen y otras técnicas populares.

Las organizaciones de seguridad están mejorando en la investigación de delitos en línea y utilizando mejores tácticas con más recursos destinados contra el crimen digital.

Las comunicaciones deben estar cifradas y nuestra privacidad

debe protegerse para generar una mejor ciberseguridad. Telegram puede y ya ha filtrado algunas palabras clave que no se pueden, pero la forma en que la comunidad criminal evita esto es creando nuevas palabras para que los productos y servicios permanezcan en la búsqueda.

“Lamentablemente, donde hay un mercado, siempre habrá una manera. Telegram y algunos otros servicios de redes sociales probablemente continuarán siendo utilizados para el mercado ilegal. Con el software y las técnicas ahora ampliamente disponibles, para incluso borrar cualquier indicio de evidencia, es claro que estamos eliminando lentamente cualquier posibilidad de que esto llegue a una solución en el corto plazo. Las plataformas que ofrecen privacidad siempre serán aprovechadas por aquellos que quieran esconderse en las sombras, por lo cual es vital que todos seamos conscientes del problema.”, concluyen desde ESET.

Con información de Banca y Negocio.