13 marzo 2019 16:35

Il dark web si sposta su app molto popolari per vendere meglio le droghe

di Redazione

Gli spacciatori di dark web usano app famose per vendere i propri prodotti, spesso usando i graffiti stradali per pubblicizzare i propri account ai clienti e bot automatizzati per comunicare con loro.
La questione è soggetta ad un giro di vite sui mercati online illegali, mentre l'introduzione della crittografia nelle app consente agli utenti di rimanere anonimi.
Esperti informatici hanno osservato questa crescente tendenza tra i criminali clandestini, rilevando come vengano utilizzate tattiche innovative per sfuggire ai rilevamenti della polizia.
Parlando in modo anonimo al quotidiano The Independent, un ricercatore del dark web che ha attivato alcuni di questi canali nell'app di messaggistica Telegram, ha spiegato come i bot automatizzati sono utilizzati per comunicare con i clienti - sia per comodità che per evitare di farsi individuare.
Il ricercatore ha usato le immagini dei nomi dei canali scrivendoli con vernice a spruzzo sui muri vicino a stazioni di trasporti e altri luoghi pubblici per pubblicizzare questi canali a potenziali clienti.
Un altro importante cambiamento nel modo in cui operano questi spacciatori è l'uso di "dead drops” (gocce morte) (1) per distribuire il prodotto. Questo evita i pericoli dell'incontro faccia a faccia, nonché anche il rischio che le droghe vengano rintracciate o intercettate attraverso il sistema postale.
Le merci sono invece nascoste in luoghi accessibili al pubblico, come i parchi, prima che l’ubicazione venga inviata al cliente una volta che l'acquisto è stato effettuato. Cptovalute semi anonime come bitcoin facilitano i pagamenti.
Le dropgangs, come sono state soprannominate, sono stati scoperte per la prima volta in Ucraina, ma da allora sono stati individuati in Russia, nei Balcani e in gran parte dell'Europa centrale e orientale.
Il consulente speciale di Europol Rik Ferguson si riferisce alla crittografia end-to-end e ai limitati controlli di identità che rendono le app come Telegram attraenti per le gang.
"I criminali operano sempre più come le aziende d’oggi e hanno bisogno di strumenti di comunicazione affidabili per portare a termine il loro lavoro", ha dichiarato a The Independent Ferguson, che è anche a capo della ricerca nella società di sicurezza informatica Trend Micro.
"Telegram è diventato lo strumento preferito dai i criminali, ma non è la prima app ad essere utilizzata in questo modo. Canali come WhatsApp e Facebook Messenger hanno avuto le loro glorie nella malavita criminale, quindi Telegram probabilmente non sarà l'ultimo".
Telegram in precedenza aveva guadagnato notorietà dopo essere diventato lo strumento di comunicazione scelto dall'Isis, ma, da allora c'è stata una repressione significativa sui canali che ospitano attività terroristiche.
Più di recente, un'indagine ha scoperto immagini di pedofilia e il furto di numeri di carte di credito scambiati apertamente tramite Telegram - ancora una volta indicando la tendenza delle app criptate che prendono il posto del dark web come luogo di messa in opera deò crimine.
"Le app di crittografia sono avviate con buone intenzioni, come aiutare a proteggere le comunicazioni private dallo spionaggio del governo", ha dichiarato Boris Cipot, un ingegnere addetto alla sicurezza presso la società di software Synopsys. "Ma, sfortunatamente, anche se questa funzionalità è stata creata per un buon uso, ci sono

quelli che ne abuseranno sempre per ragioni negative."
Telegram non ha risposto a diverse richieste di commenti, anche se in precedenza ha dichiarato di essere impegnato in "ricerche specifiche" per trovare e rimuovere attività illegali sulla sua piattaforma.
Nonostante la proliferazione di dropgangs e le difficoltà incontrate dalle autorità nel rintracciarle e fermarle, gli esperti di sicurezza avvertono che sarebbe pericoloso forzare app come Telegram a compromettere la crittografia che usano.
"Il problema non sarà risolto da quei governi che chiedono l'installazione di backdoor nel software per consentirne l'accesso", ha dichiarato il consigliere di Europol Rik Ferguson.
"Questo servirebbe solo a minare fondamentalmente la crittografia - le backdoor non hanno garanzie e aprono le comunicazioni dei consumatori a un nuovo mondo di attacchi".

(articolo di Anthony Cuthbertson, pubblicato sul quotidiano The Independent del 13/03/2019)

NOTA
1 – ndr: L'USB dead drop (gocce morte) è un sistema di file sharing offline, peer-to-peer e anonimo, creato dall'artista tedesco Aram Bartholl, che consiste nella condivisione pubblica di chiavette USB in spazi aperti. Nel caso più tipico, la chiave USB viene inserita in un muro e fissata con cemento a presa rapida.