**Check Point: Telegram nowym kanałem dla cyberprzestępców**

**Dark Web nie jest już jedynym ulem działań półświatka cyberprzestępczego. Jak odkrył zespół badawczy firmy Check Point Software Technologies, zamknięcie takich rynków dark webu jak Hansa Market i Alpha Bay, przez organy ścigania w USA i Europie, doprowadziło do przeniesienia się przestępców na zupełnie inny, nowy kanał dystrybucji! Aby uniknąć interwencji organów ścigania przestępcy kontynuują swoją działalność korzystając z szyfrowanej aplikacji mobilnej Telegram.**

Fora dark netu są popularną platformą komunikacyjną wśród przestępców do promocji swoich usług, a nawet ich konsultacji poszczególnych działań między sobą. Jednak w ostatnich kilku latach, gdy organy ścigania lepiej rozumieją wyzwania z którymi się borykają, nacisk władz na fora uległ wzmocnieniu, a niektóre z nich zostały zamknięte. W rezultacie obecnie ma miejsce migracja na bardziej tajemniczą i łatwo dostępną platformę.

Telegram jest aplikacją pozwalającą na bezpośrednią, szybką komunikację dzięki zaszyfrowanym wiadomościom. Zaprezentowana w 2013 roku, odnotowała po awarii serwerów WhatsAppa niesamowity wzrost użytkowników – w zaledwie 24 godziny przybyło ich aż pięć milionów!

Podobnie jak w przypadku aplikacji WhatsApp, użytkownicy programu Telegram mogą rozmawiać zarówno z osobami indywidualnymi, jak i z grupami. Cechami wyróżniającymi go spośród innych jest bezpieczeństwo i anonimowość. W rezultacie, niektóre z jego hostowanych grup czatu stały się użyteczną alternatywą dla tajnych forów w tzw. ciemnej sieci, informuje firma Check Point na swoim blogu.

Grupy dyskusyjne hostowane przez Telegram, znane jako "kanały", mogą być używane do rozsyłania wiadomości o w zasadzie nieograniczonej liczbie subskrybentów z jednoczesnym zachowaniem dużej dyskrecji dzięki odpowiedziom z pominięciem innych użytkowników oraz szyfrowaniu wiadomości.

W przeszłości należało wykonać kilka kroków by połączyć się z darknetem za pośrednictwem platformy TOR. Dziś każdy użytkownik Telegrama może dołączyć do podejrzanych lub mówiąc wprost – nielegalnych kanałów, dzięki jednemu kliknięciu w telefonie, zachowując przy tym pełną anonimowość.

**Telegram: kanały nielegalne**

Przykładami są np. kanały „Dark Jobs”, „Dark Work” oraz “Black Market”, choć, jak informuje Check Point, jest ich zdecydowanie więcej. Dla przykładu „Dark Jobes” oferuje płatne „prace” czy też zadania, które są uszeregowane kolorami – czarne związane są z wysokim ryzykiem prawnym; szare i białe są mniej niebezpieczne.

Kanały te nie ograniczają się jednak wyłącznie do komunikacji między rekruterami a osobami poszukującymi zarobków. Można tu również znaleźć reklamy sprzedaży skradzionych dokumentów lub narzędzi hakerskich. Jest to szczególnie niepokojące, biorąc pod uwagę dostępność kanałów oraz częste obietnice wysokich wynagrodzeń.

W rezultacie stwarza to ryzyko wzrostu wskaźnika cyberprzestępczości, ponieważ propozycje te są nie tylko otwarcie wprowadzane na rynek, ale również dostępne dla niedoświadczonych użytkowników, dzięki czemu niebezpieczne narzędzia są teraz w zasięgu niemal każdego.

Najciekawszymi wydają się być te wiadomości, w których poszukuje się pracowników w określonych firmach i bankach. Przestępcy chcą wykorzystywać personel do uzyskania poufnych danych, które mogą być następnie wykorzystane do celów osobistych, sprzedaży lub przeprowadzenia cyberataku z wnętrza firmy. Podobnie jak w świecie rzeczywistym, w świecie cyberprzestępczości nie jest ważne to co wiesz, ale to kogo znasz…

Inną nielegalną usługą w kanałach Telegramu jest np. fałszowanie dokumentów prawnych. Podrobione dokumenty obejmują m.in. dowody tożsamości, paszporty czy dokumenty bankowe. Autor jednego z kanałów twierdzi nawet, że ma kontakty wewnątrz wydziału drogowego rosyjskiej policji i ma możliwość wydawania lub aktualizowania praw jazdy wszystkich kategorii.

Wygoda kanałów aplikacji Telegram umożliwia bezpieczniejszą i łatwiej dostępną komunikację między podmiotami stanowiącymi zagrożenie oraz podmiotami pragnącymi uczestniczyć w cyberprzestępstwach.

Choć z biegiem lat komunikatory stały się integralną częścią współczesnego życia i były udoskonalane w celu zapewnienia bezpieczeństwa informacji o użytkownikach, są one również wykorzystywane przez tych, którzy uciekają przed prawem. Dzięki takim narzędziom kwitnie nielegalny handel, dostęp do złośliwego oprogramowania nigdy nie był łatwiejszy, a firmy mogą być zagrożone przez własnych pracowników.

Obecnie dzięki powszechnej dostępności tego typu kanałów oraz coraz prostszym narzędziom hakerskim, liczba podmiotów stanowiących zagrożenie rośnie, a w parze z tym idzie liczba ataków cybernetycznych, zarówno na organizacje, jak i na osoby fizyczne.