



OSTRZEGAMY PRZED OSZUSTAMI PODAJĄCYMI SIĘ ZA BROKERÓW FINANSOWYCH. MATERIAŁ WIDEO.

Inwestowanie staje się coraz prostsze. Przez internet możemy m.in. obracać akcjami giełdowymi, inwestować w kryptowaluty. Na fali popularności tej formy inwestycji, za pomocą zarejestrowanych za granicą fałszywych stron internetowych i socjotechniki, oszuści podszywają się pod brokerów finansowych oferując spektakularne wręcz zyski. Na podstawie materiałów śledztwa Wydziału do walki z Cyberprzestępczością KWP w Krakowie dotyczącego platformy www.globalmaxis.com prezentujemy spot ostrzegający przed tego typu wyłudzeniami.



Wraz z rozwojem technologii informatycznych inwestowanie staje się bardziej dostępne i coraz prostsze. Przez internet możemy m.in. obracać akcjami giełdowymi, inwestować w waluty i różnice giełdowe na rynku Forex, w metale szlachetne, czy kupować kryptowaluty. Na fali popularności inwestowania przez internet próbują wzbogacić się także oszuści. Za pomocą zarejestrowanych za granicą fałszywych stron internetowych i zmyślnej socjotechniki, podszywają się pod brokerów finansowych oferując spektakularne wręcz zyski, i to bez ryzyka. Usługi tych pseudobrokerów często są reklamowane w mediach społecznościowych, serwisach internetowych oraz aplikacjach mobilnych. W reklamach nierzadko korzystają z dostępnych w sieci zdjęć osób cieszących się dużym zaufaniem społecznym czy celebrytów. Firmy, w których pracują oszuści, mimo że okradają ludzi, często działają legalnie. Zarejestrowane są w tropikalnych rajach podatkowych, a ich pracownicy dostają regularne wypłaty oraz premie za wyniki. Jednak ich przedstawicielstwa, biura w Polsce widnieją tylko „na papierze”.

Oszuści podkreślają, że potencjalny klient nie musi znać się na rynkach finansowych, obsłudze specjalistycznych serwisów, czy śledzić kursy akcji. Ba, nie musi nawet być biegły w obsłudze komputera, czy smartfonu. Wystarczy, że skorzysta z ich „pomocy”. Pseudobrokerzy namawiają ofiary by wykonywały podawane przez telefon polecenia, bądź instalowały oprogramowanie do tzw. zdalnego pulpitu i przekazywały telefonicznym „konsultantom” uprawnienia do sterowania swoim komputerem, tabletem bądź telefonem. Dzięki temu przestępcy sięgają do kont bankowych bądź zaciągają pożyczki bankowe na nazwisko ofiary. Obecnie w mediach dużo się mówi o kradzieży tożsamości w celu wyłudzenia kredytów, czy dokonywania oszustw. Paradoksalnie, w tym przypadku ofiara sama, daje dostęp oszustowi do swojej tożsamości.

Na podanej powyżej zasadzie działali także oszuści z platformy www.globalmaxis.com, którzy spowodowali straty finansowe u kilkuset osób w Polsce. Prokuratura Okręgowa w Krakowie, na polecenie Prokuratury Krajowej, nadzoruje śledztwo prowadzone przez policjantów z Wydziału do walki z Cyberprzestępczością KWP w Krakowie. Do śledztwa tego

włączono postępowania z całego kraju, dotyczące ponad 300 osób pokrzywdzonych przez pseudobrokerów z „globalmaxis.com”. Policjanci prowadzą tą sprawę pod kątem wielokrotnych oszustw na znaczną kwotę.

Z procederu oszuści uczynili sobie stałe źródło dochodu (art. 286 § 1 kk w zw. z art. 294 § 1 kk w zw. z art. 12 § 1 kk i w zw. z art. 65 § 1 kk), bezprawne przetwarzając, gromadząc lub przekazując dane informatyczne oszukanych osób (art. 287 § 1 kk w zw. 12 § 1 kk kk i w zw. z art. 65 § 1 kk) oraz „piorąc” pieniądze (art. 299 § 1 i 5 kk w zw. z art. 12 § 1 kk). Obecnie czynności śledztwa skupiają się na czynnościach wykrywczych i dowodowych. Sprawcom grozi nawet do 10 lat pozbawienia wolności.

Jak ustalono, osoby pokrzywdzone, skuszone za pomocą reklam w sieci Internet, perspektywą stosunkowo łatwego zarobku, założyły konta użytkowników na stronie internetowej www.globalmaxis.com zarejestrowanej na rzecz spółki działającej w jednym z tropikalnych rajów podatkowych. Następnie kontaktowali się z nimi „konsultanci” tej „firmy”, telefonicznie instruując co do zainstalowania na komputerach, bądź telefonach komórkowych oprogramowania do obsługi tzw. pulpitu zdalnego (np. AnyDesk).

Za pomocą tego oprogramowania sprawcy przejęli kontrolę nad urządzeniami inwestorów i uzyskali dostęp do systemów bankowości elektronicznej obsługującej rachunki tych pokrzywdzonych, by bez ich wiedzy i zgody dokonać transakcji bankowych na przejęte w ten sam sposób konta innych pokrzywdzonych, skąd środki ostatecznie trafiały poza granice Polski i Europejskiego Obszaru Gospodarczego w formie przelewu lub wypłaty gotówkowej.

Zaznaczyć jednak należy, że według wiedzy zgromadzonej w toku dotychczasowego śledztwa, sprawcy o podobnym sposobie działania jak opisany wyżej, mogą posługiwać się innymi nazwami platform pseudoinwestycyjnych.

Na podstawie materiałów tego postępowania prezentujemy spot ostrzegający przed wyłudzeniami, przygotowany przez zespół prasowy KWP w Krakowie we współpracy ze śledczymi.

Dodać należy, że Komenda Główna Policji i FinCERT.pl – Bankowe Centrum Cyberbezpieczeństwa ZBP ostrzegały już kilkakrotnie przed próbami oszustw przy inwestowaniu w kryptowaluty oraz na rynku Forex. ([link do policja.pl](http://link.do.policja.pl)). Podobne sprawy, dotyczące innych pseudobrokerów, prowadzą także komendy wojewódzkie Policji w kraju (np. KWP w Rzeszowie: [link do strony podkarpackiej policji](http://link.do.strony.podkarpackiej.policji)).