Artykuł: **Przestępstwo „*na blika*”**

„*Dzień Dobry.*

Chciałbym zgłosić przypuszczalne przestępstwo wyłudzenia.

Straciłem 900 złotych tj. pieniądze zostały wypłacone z mojego konta. tzn. ja je przelałem, ale nie tej osobie, której chciałem przekazać gotówkę”

– początkowo nieskładne, enigmatyczne dla przyjmującego, składane wyjaśnienie przez pokrzywdzonego.

„*Teraz wiem, że ktoś się podszył pod mojego kolegę Jarka i kontaktując się ze mną poprzez komunikator Messenger, poprosił mnie o przelanie tej kwoty. Tzn. oczywiście nie Jarek tylko ten ktoś trzeci. Dlaczego to zrobiłem? Zawsze tak z Jarkiem robimy, pożyczając sobie kasę, gdy pieniędzy brakuje. Do tej pory wszystko było OK. Usługa BLIK jest bardzo wygodna. Można nią przenosić pieniądze na telefon znajomego i nawet wykorzystać do tego celu bankomat. Dopiero po telefonie Jarka zorientowałem się, że nie jemu podałem kod BLIK tylko innej osobie, która w jakiś sposób pozyskała dane Jarka. Może włamano się do jego komputera, a może do mojego. Nie wiem Szkoda, że wtedy nie pomyślałem, Po prostu byłem naiwny . Powinienem zadzwonić do kolegi i potwierdzić, że to on napisał do mnie tę wiadomość. Nie wiedziałam, że ktoś może podszyć się po niego. Nie wiem w jaki sposób, ale doprowadził do tego, przekonał mnie, że podałem kod do wypłaty. Gdyby przynajmniej byłby to przelew klasyczny to może zdążyłbym zablokować środki, a tak przepadło. Kto to zrobił? Jak to się mogło właściwie stać?*”

Takie pytania pojawiają się coraz częściej, m.in. przy zgłoszeniach o podejrzeniu popełnienia przestępstwa „na blika” (zdjęcie poniżej)

Prawidlowy numer to

Dnia 19 listopada 2019 18:42 Joanna K napisał(a):

Dobry wieczor,

Dzis o 17:46 z bankomatu Euronet ul. Rynek 29 we Wroclawiu wyludzono ode mnie 1000zl tzw metoda "na blika". Sprawca podszyl sie pod moja kolezanke i napisal na facebooku, ze potrzebuje kod do wykonania transakcji. Jako, ze obie mieszkamy poza Polska, wiem ze czasem miewamy takie problemy, wiec bez zbednych pytan podalam kod. Wiem, moja wina i prawie niemozliwym jest zlapac przestepce, ale mam nadzieje, ze zgloszenie pomoze ostrzec innych. W zalaczaniu zdjecie wykonanej transakcji.

Pozdrawiam,

Joanna K

Sama usługa moim zdaniem jest bardzo wygodna i prosta dla użytkownika. Jest bardzo popularna wśród młodych ludzi. Jest również doskonałym rozwiązaniem dla naszych pociech w przypadku gdy na wakacjach zabraknie pieniędzy i wystąpi potrzeba szybkiego przelewu. Co wtedy? Prośba o kod BLIK, wynegocjowana kwota i najbliższy bankomat z usługą wypłat BLIK. Istnieje również przelew na telefon BLIK, ale o tym może następnym razem. Wszystko by było dobrze gdyby wypłatę poprzedził kontakt telefoniczny np. tak jak w przypadku rozrzutnego kolonisty. Natomiast w sytuacji tylko kontaktu wirtualnego ryzyko jest wyższe i jak widać po statystykach, zagrożenie całkiem realne. Wirtualizacja komunikacji jest szybka i wygodna, ale niesie za sobą ryzyko podszycia się pod inną osobę. Przez „pisanego” Messengera przecież nie sprawdzimy, kto jest po drugiej stronie i czy faktycznie jest to nasz znajomy.

Na czym polega przestępstwo „na blika”? Na co zwracać uwagę? Jakie mechanizmy są wykorzystywane przez przestępców?

O tym w poniżej.

Użytkownicy szybko przyzwyczaili się do wygody wynikającej

z wykorzystywania usług elektronicznych, takich jak: płatności elektroniczne, przelewy, zakupy, wymiana informacji, łatwość i szybkość dostępu do danych itp.

Cieszymy się z szybkości przeprowadzanych transakcji, z wygody i prostoty ich wykonywania, co w efekcie daje nam sporą oszczędność czasu. Niestety, często zapominamy o tym, że istnieje również ciemna strona sieci. Podszywanie się pod innych, tworzenie „fałszywej" – wirtualnej tożsamości, stało się już tak nagminne, że szanujący się usługodawcy wprowadzili i stale modyfikują procesy personalizacji tj. zabezpieczenia użytkownika przed niebezpieczeństwami czyhającymi w sieci, również ochroną przed … nim samym. Najprostszym przykładem takich działań jest wprowadzenie przez banki przy bankowości elektroniczną dwustopniowego systemu weryfikacji dostępu. Początkowo do zalogowania się do naszych kont wystarczył login i hasło, jednak niefrasobliwość samych użytkowników i w konsekwencji przejmowanie ich tożsamości przez sprawców cyberprzestępstw , doprowadziły do uszczelnienie tego procesu przez banki. Warto tutaj wspomnieć, iż Policja Dolnośląska w latach 2001-2005 miała decydujący wkład w przekonanie instytucji bankowych o konieczności poprawy procesu personalizacji tj. wprowadzenie dwustopniowego procesu weryfikacji tożsamości użytkownika.

Głównym „paliwem" w przestępczości skierowanej przeciwko usługom elektronicznym jest wykorzystanie przez sprawców mechanizmów bazujących na socjotechnice.

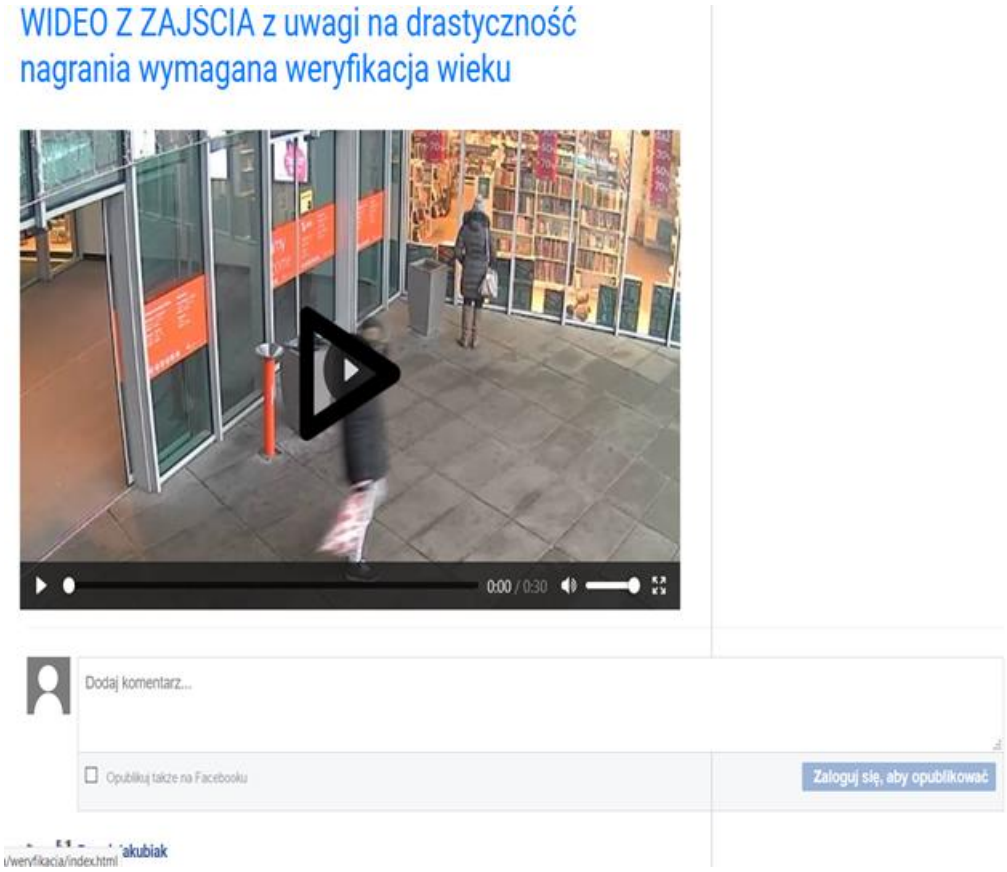
W przestępstwie spoofingu metoda przestępcza polega na podszyciu się pod nadawcę wiadomości e-mail. Musimy pamiętać, że mimo niewzbudzającego podejrzeń adresu e-mail, z jakiego wysyłana jest wiadomość elektroniczna, istnieją narzędzia do stworzenia pozoru rzeczywistego nadawcy, co pozwala sprawcy – autorowi treści, podszyć się pod nadawcę wiadomości i przemycić złośliwy kod w załączniku. Zanim zaczniemy odpowiadać na treści zawarte w takiej wiadomości lub otworzymy załącznik powinniśmy skorzystać z alternatywnego kanału komunikacji, celem ustalenia, że autorem wiadomości jest faktycznie e-mail'lowy nadawca.

W przypadku komunikatorów internetowych takich jak np. Messenger trochę inaczej wygląda mechanizm przestępczy. Podszycie się pod autora wiadomości nie jest już takie proste i wymaga wcześniejszego procesu pozyskania danych służących do zalogowania

się na Facebooka. W tym przypadku sprawcy również wykorzystują, niestety często z zamierzonym przez nich efektem, zabiegi bazujące na inżynierii społecznej. Ciekawość użytkownika sieci połączona z brakiem wiedzy na temat aktualnych zagrożeń, jest wstępem do całego łańcucha następujących po sobie okoliczności, które ostatecznie mogą doprowadzić do zachwiania właściwego poziomu bezpieczeństwa „twierdzy" użytkownika.

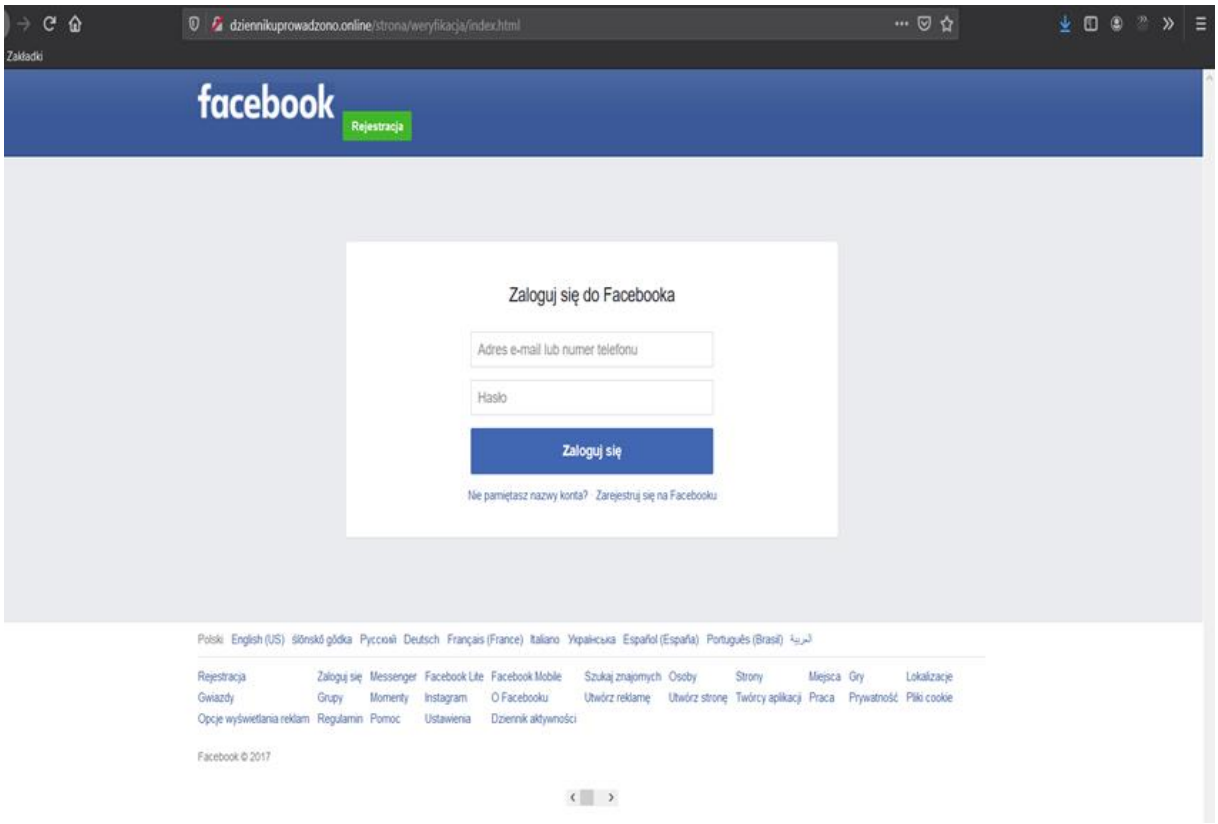
Przechodząc do sedna, bo przecież ten materiał powinien być poświęcony przede wszystkim przestępstwu „na blika" przysłowiowym początkiem końca jest przede wszystkim ciekawość użytkownika połączona z wyłączeniem wyobraźni i czasami zdrowego rozsądku. Zaczyna się od odnalezienia jakiejś sensacyjnej wiadomości, na dziwnym, niesprawdzonym portalu. Na stronie znajduje się np. film dotyczący zarejestrowanego kamerą przemysłową porwania kilkuletniego dziecka z galerii handlowej (zdjęcie poniżej).

Już w tym momencie powinna nam się zapalić przysłowiowa czerwona lampka, sygnalizująca dziwny adres strony, na której materiał się znajduje. Ciekawość Internauty pcha go dalej tj. jest zachęcony do kliknięcia w trójkącik uruchamiający materiał wideo (zdjęcie poniżej),

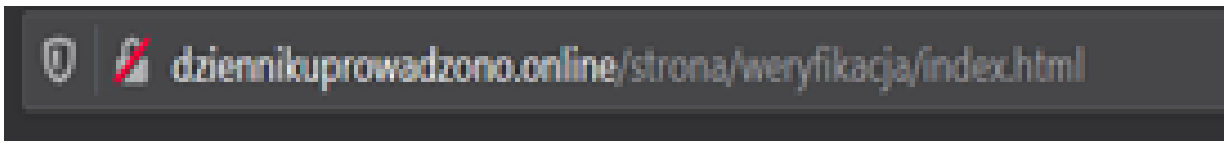


ale tutaj o dziwo, strona przekierowuje nas w następne miejsce, które ma za zadanie zweryfikowanie naszego wieku.

Wizualnie wydaje się, że przekierowanie prowadzi do strony logowania na Facebooku. Grafika ta sama, okienka proszące o login i hasło identyczne, nic podejrzanego (zdjęcie poniżej).



Wytrawny i ostrożny użytkownik zwróci jednak uwagę, że adres strony wyświetlanej różni się zupełnie od adresu oficjalnej strony. Nie wszyscy jednak tacy rozważni. Wielka szkoda (zdjęcie poniżej)



I tutaj zaczyna się właściwa aktywność przestępcy. Po pozyskaniu danych (specjalny protokół zbiera i gromadzi w chmurze dane zawierające loginy i hasła) sprawca hackingu loguje się na nasze konto facebook'owe i po analizie treści korespondencji, a ma dostęp do całości, potrafi ocenić nasze zwyczaje, ustalić dane personalne naszych dobrych znajomych i w konsekwencji, bez naszej wiedzy wysyłać do nich różne wiadomości. Również te dotyczące zapytań o nasze dane osobowe, zainteresowania oraz o możliwość pożyczki tj. przelew BLIK.

Interesującym z punktu widzenia procesowego jest to, że przestępstwo „na blika" wypełnia znamiona dwóch czynów zabronionych: przestępstwa hackingu , tj. wejścia przez sprawcą bez uprawnień w posiadanie informacji dla niego nieprzeznaczonej poprzez przełamanie lub obejście elektronicznych zabezpieczeń (art. 267 par. 1 KK), oraz

przestępstwa oszustwa - wyłudzenia środków finansowych (art. 286 par. 1).

Efekty przestępczej działalności widoczne są przede wszystkim poprzez oddziaływanie na pokrzywdzonych przestępstwem oszustwa. Pokrzywdzony działalnością hackera dowiaduje się, że padł ofiarą dopiero po sygnale od jego znajomych lub od policjanta prowadzącego postępowanie.

Na końcu wypada umieścić podsumowanie. Może lepiej prośbę skierowaną do wszystkich użytkowników sieci. Prośbę o rozwagę połączoną z bardzo umiarkowaną ekscytacją wszystkim, czym karmimy się w Internecie tj.: „gorącymi" wiadomościami, pogonią za sensacją, usilnym ale i naiwnym poszukiwaniem znajomych, nierozważną ucieczką przed samotnością, wiara we wszystko, co przychodzi do nas drogą elektroniczną i zaufaniem w źródło pochodzenia tych wiadomości.

Pamiętajmy również, że wraz ze wzrostem ilości użytkowników sieci Internet, wzrasta również zainteresowanie wszystkim, co jest związane z tym medium przez zorganizowane grupy przestępcze, zachęcone łatwością wprowadzenia w błąd nawet bardzo wytrawnych użytkowników zasobów internetowych. Nie unikajmy relacji face to face, ponieważ to może niekiedy ochronić nas przed czyhającymi niebezpieczeństwami.

autor artykułu:

mł. insp. Ryszard Piotrowski

- Naczelnik Wydziału dw. z Cyberprzestępczością KWP we Wrocławiu

- biegły sądowy przy Sądzie Okręgowym we Wrocławiu z dziedziny Cyberprzestępczości