PODSUMOWANIE ATAKÓW

PHISHING

SZYBKIE PŁATNOŚCI 2018

CZYTANIE ZAJMIE 9 MINUT



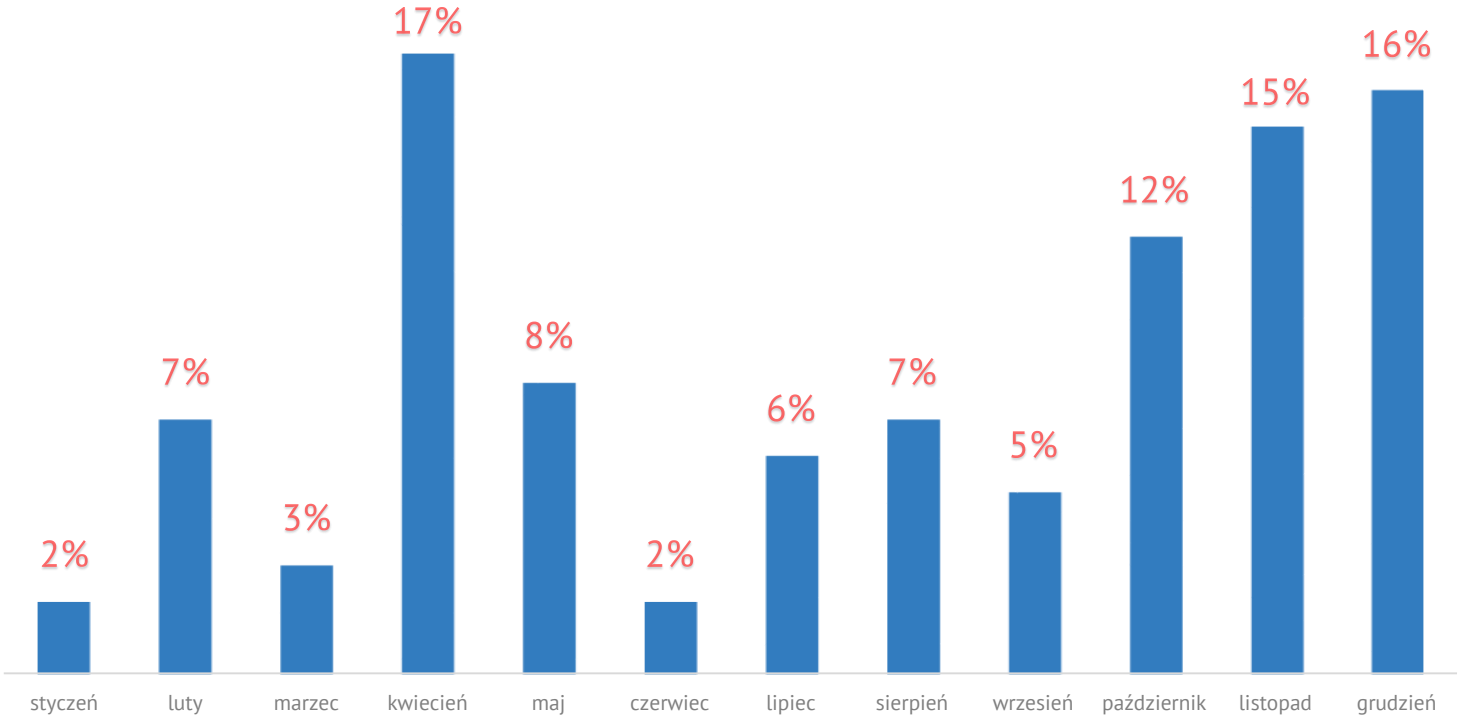
PREBYTES
SECURITY INCIDENT RESPONSE TEAM

SZYBKIE PŁATNOŚCI

PODSUMOWANIE ATAKÓW PHISHING WYKORZYSTUJĄCYCH FAŁSZYWE STRONY SZYBKICH PŁATNOŚCI W 2018 ROKU

Raport przedstawia skalę ataków phishing z wykorzystaniem fałszywych stron szybkich płatności. Jest to podsumowanie ataków, które miały miejsce w 2018 roku. Za ich pośrednictwem cyberprzestępcy wykradali poufne dane użytkowników bankowości internetowej. Schematy ataków były różne, jednak przestępcy zawsze wyłudzali informacje, dzięki którym mogli uzyskać dostęp do konta bankowego ofiary i wypłacić z niego pieniądze.

Natężenie ataków phishing w poszczególnych miesiącach 2018 roku



PHISHING

To oszustwo polegające na podszywaniu się pod legalnie działające organizacje lub osoby prywatne, w celu wyłudzenia poufnych danych.

Phishing obejmuje kradzież numerów kart płatniczych, haseł dostępu do bankowości i serwisów internetowych oraz innych poufnych danych.



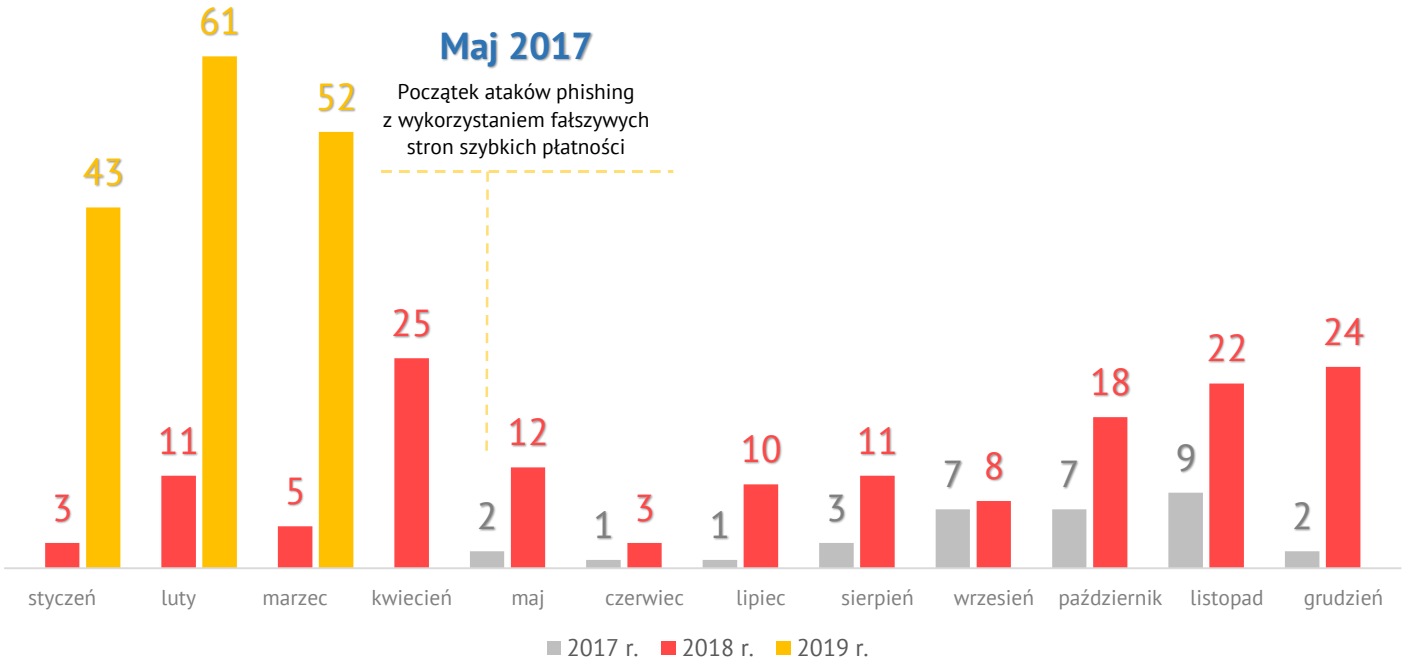
Ataki phishing wykorzystujące fałszywe strony szybkich płatności zaczęły się w maju 2017. W tym czasie zaobserwowaliśmy nowy trend w atakach phishing ukierunkowanych na polskie bankowości internetowe. Przez cały 2018 rok cyberprzestępcy kontynuowali ataki oraz tworzyli nowe taktyki wyłudzania danych. PREBYTES SIRT wykrył i zablokował w 2018 roku 152 domeny wykorzystywane przez przestępców wyłącznie w atakach phishing z wykorzystaniem fałszywych stron szybkich płatności.



152

wykrytych i zablokowanych przez PREBYTES SIRT ataków phishing wykorzystujących fałszywe strony szybkich płatności

Porównanie liczby ataków phishing w 2017, 2018 i 2019 roku





W każdym przypadku strony phishing korzystały z certyfikatów SSL, które zapewniały poufność transmisji przesyłanych danych



Za pośrednictwem stron phishing cyberprzestępcy dystrybuowali także złośliwe aplikacje na system Android

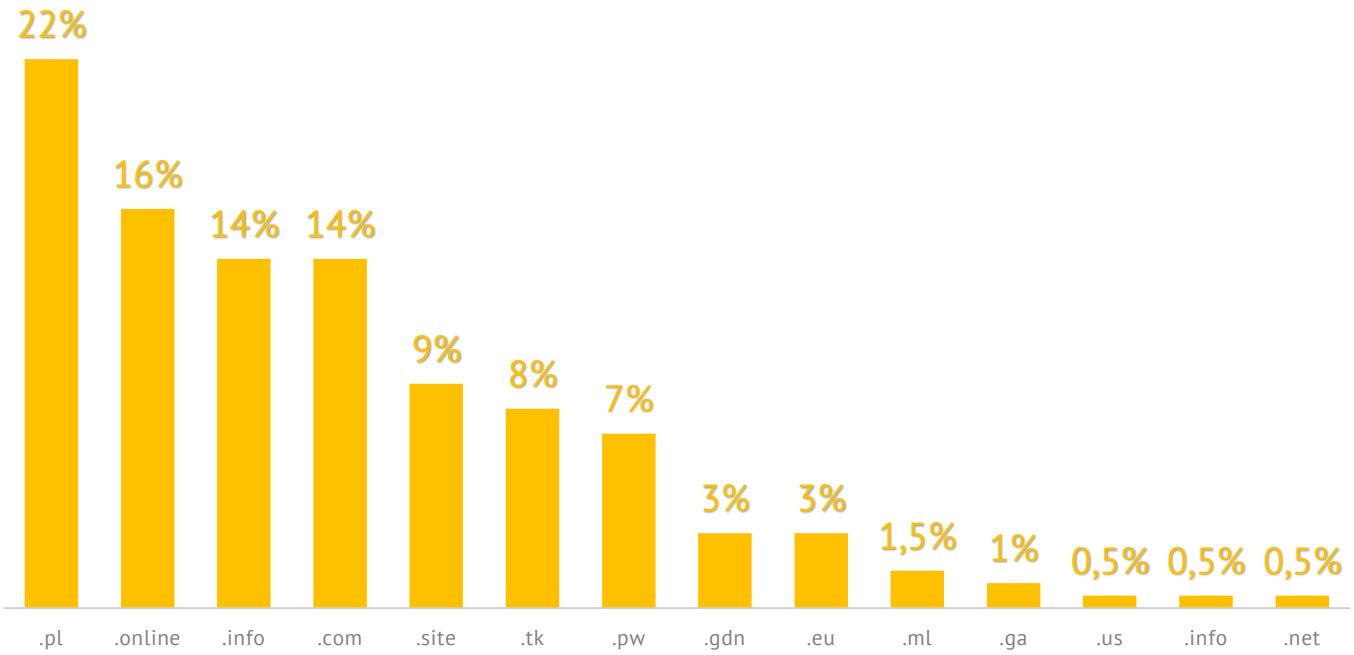


Cyberprzestępcy w atakach phishing wyłudzali także dane kart płatniczych

W celu przeprowadzenia ataku cyberprzestępcy kupują domeny o różnych TLD. Najczęściej wybierali .pl. Czasem wybierają te z mało popularnym TLD - z dwóch powodów. Są one tańsze i trudniejsze do zablokowania. Domeny .pl miały 22% udział w omawianych atakach.



Procentowy udział poszczególnych TLD domen, które służyły w omawianych atakach.



.PL to najczęściej wykorzystywane przez przestępców TLD.

Domeny z tym TLD są chętnie kupowane przezprzestępców głównie dlatego, aby zwiększyć zaufanie użytkowników do strony.



Lokalizacje serwerów stron phishing

75%	Stany Zjednoczone
9%	Polska
6%	Holandia
5%	Litwa
3%	Ukraina
1,5%	Rumunia
0,5%	Australia

W **57%** ataków phishing cyberprzestępcy ukrywali prawdziwe adresy IP domen. W tym celu korzystali z usługi **Cloudflare**.

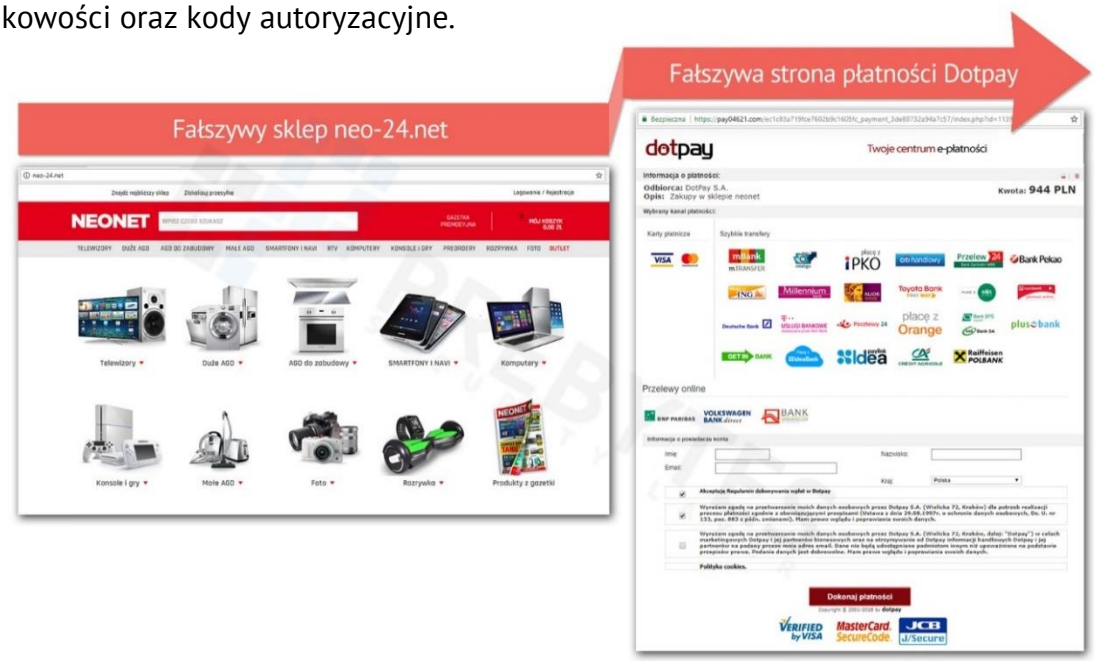
Usługa **Cloudflare** umożliwia m.in. ukrycie prawdziwego adresu IP domeny. Lokalizacja wskazuje wówczas na serwery należące do Cloudflare (Stany Zjednoczone), a nie docelowy adres IP, który może znajdować się w zupełnie innym kraju. Cyberprzestępcy chętnie korzystają z tej usługi, głównie dlatego, że zablokowanie strony phishing jest wówczas znacznie utrudnione.



JAK OFIARY TRAFIAŁY NA STRONY PHISHING

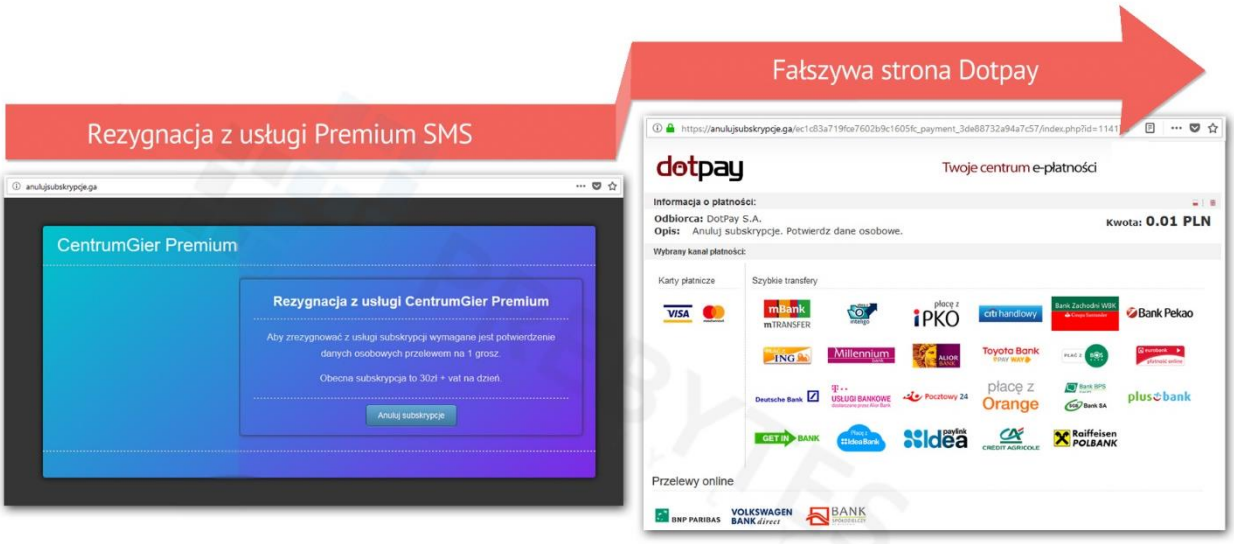
Fałszywe sklepy online

Cyberprzestępcy tworzyli własne, fikcyjne sklepy online, w których płatność za towar odbywała się za pośrednictwem fałszywych stron szybkich płatności. Ofiara chcąc zapłacić za zakupy była przekierowywana do fałszywej strony Dotpay. Po wyborze banku następowało przekierowanie do fałszywej strony banku, za pomocą, której wyłudzane były prawdziwe dane logowania do bankowości oraz kody autoryzacyjne.



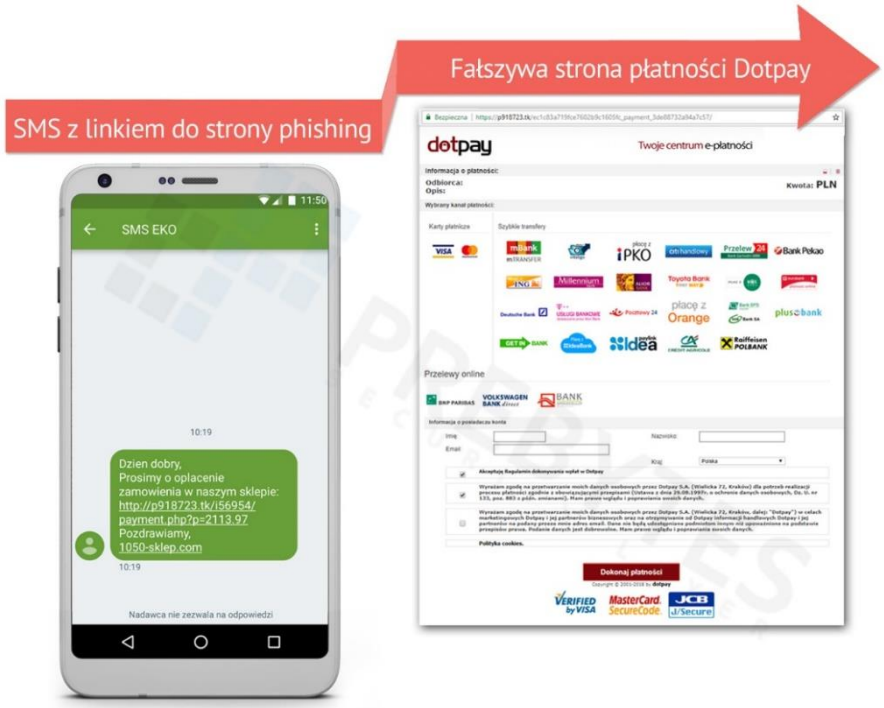
Rezygnacja z usługi CentrumGier Premium

Pod pretekstem rezygnacji z usługi CentrumGier Premium, cyberprzestępcy nakłaniali do anulowania rzekomych subskrypcji płatnych SMSów. Aby zrezygnować z subskrypcji należało potwierdzić swoje dane osobowe i w tym celu zrobić przelew na 1 grosz. Po kliknięciu w przycisk Anuluj subskrypcje następowało przekierowanie do strony phishing.



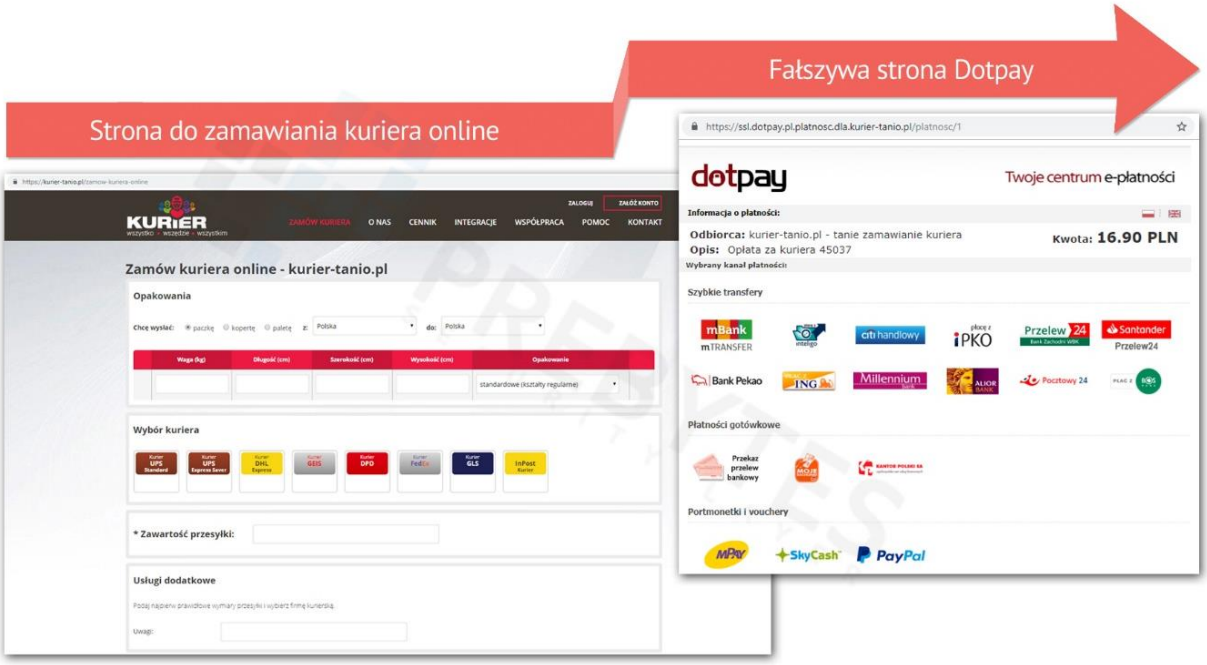
Linki w wiadomościach SMS

Linki przekierowujące do stron phishing rozsyłane były także w wiadomościach SMS. W wielu przypadkach osobami, które je otrzymywały byli Klienci fałszywych sklepów tworzonych przez cyberprzestępców. Link w wiadomości przekierowywał do fałszywej strony szybkich płatności, a po wybraniu bankowości do fałszywej strony banku.



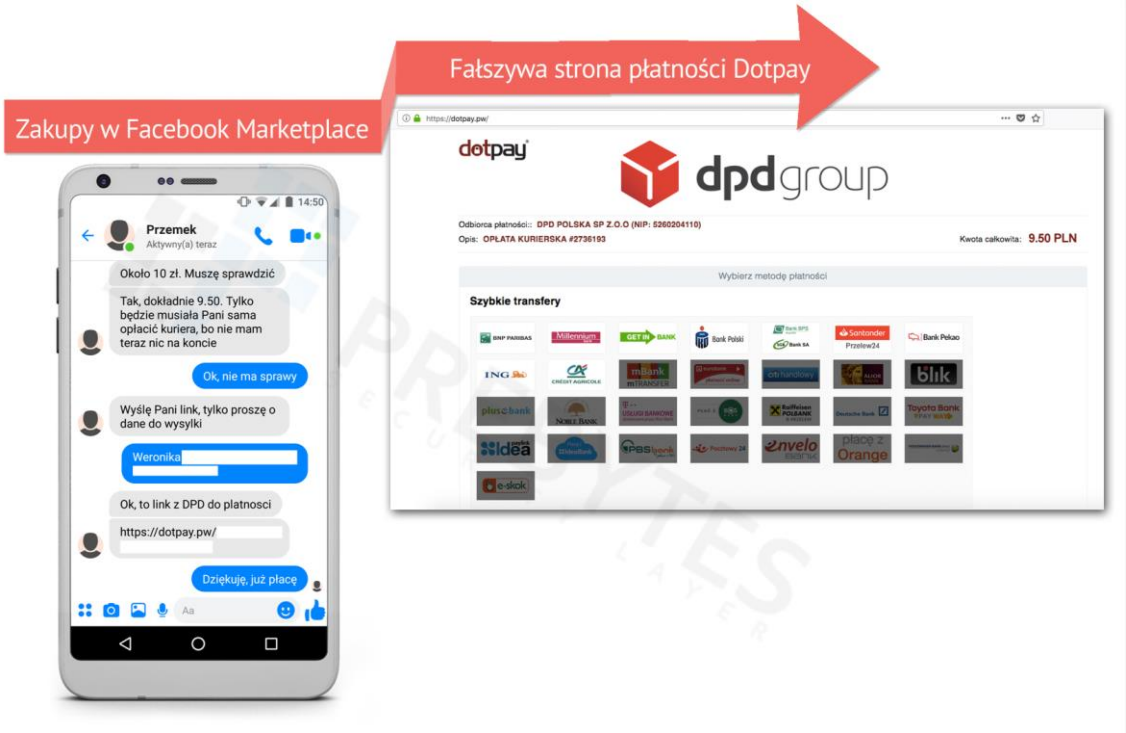
Wiadomości email z linkiem

Cyberprzestępcy rozsyłali wiadomości email podszywając się pod firmę kurierską DPD. Pod pretekstem uregulowania płatności za zamówienie nakłaniali do klikania w link, który przekierowywał do fałszywej strony szybkich płatności.



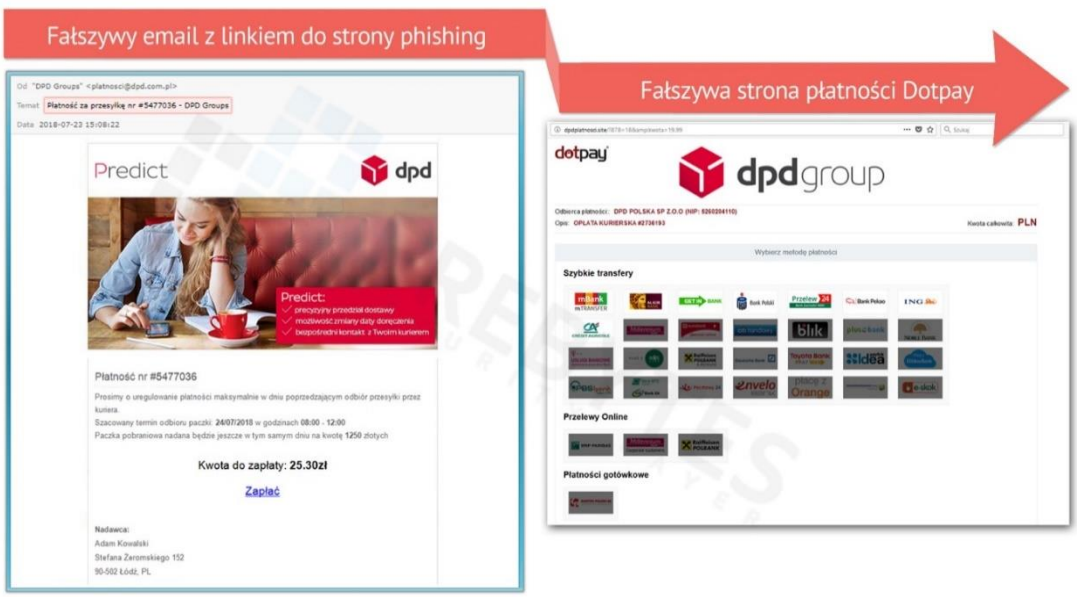
Zamawianie kuriera online

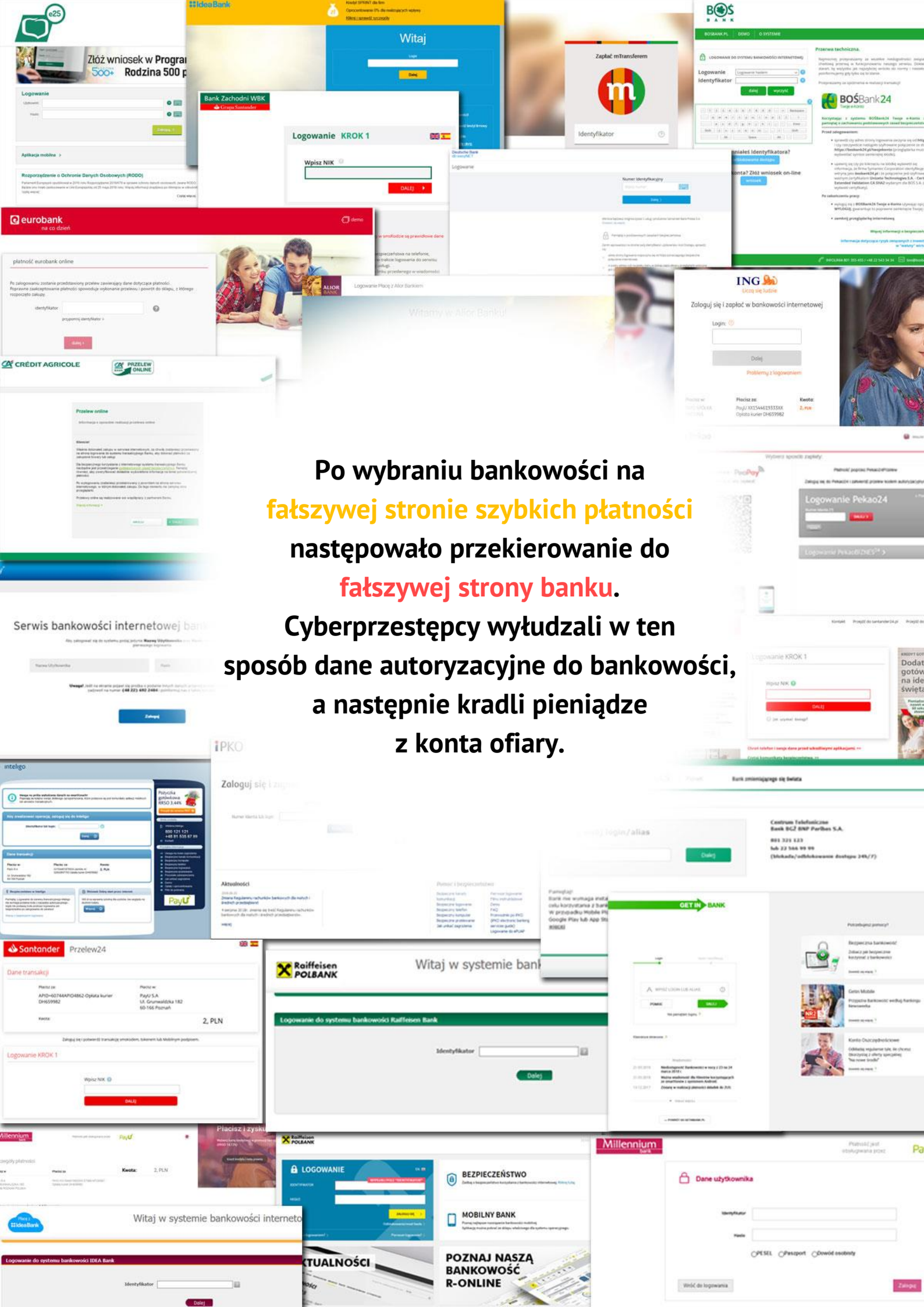
Kolejnymi stronami, które finalnie przekierowywały do fałszywej strony szybkich płatności były strony do zamawiania kuriera online. Aby zamówić kuriera należało wypełnić formularz znajdujący się na stronie. Po wybraniu wszystkich opcji oraz podaniu danych osobowych wraz z adresem dostawy należało opłacić kuriera. W tym momencie następowało przekierowanie do fałszywej strony szybkich płatności Dotpay.



Oferty sprzedaży na OLX oraz portalach społecznościowych

Cyberprzestępcy wystawiali fałszywe ogłoszenia na OLX oraz Facebook Marketplace. Podczas rozmowy z potencjalnym kupcem prosili o opłacenie kuriera. Nieświadomy użytkownik miał dokonać opłaty za pomocą fałszywej strony szybkich płatności, którą otrzymywał w wiadomości od sprzedającego.



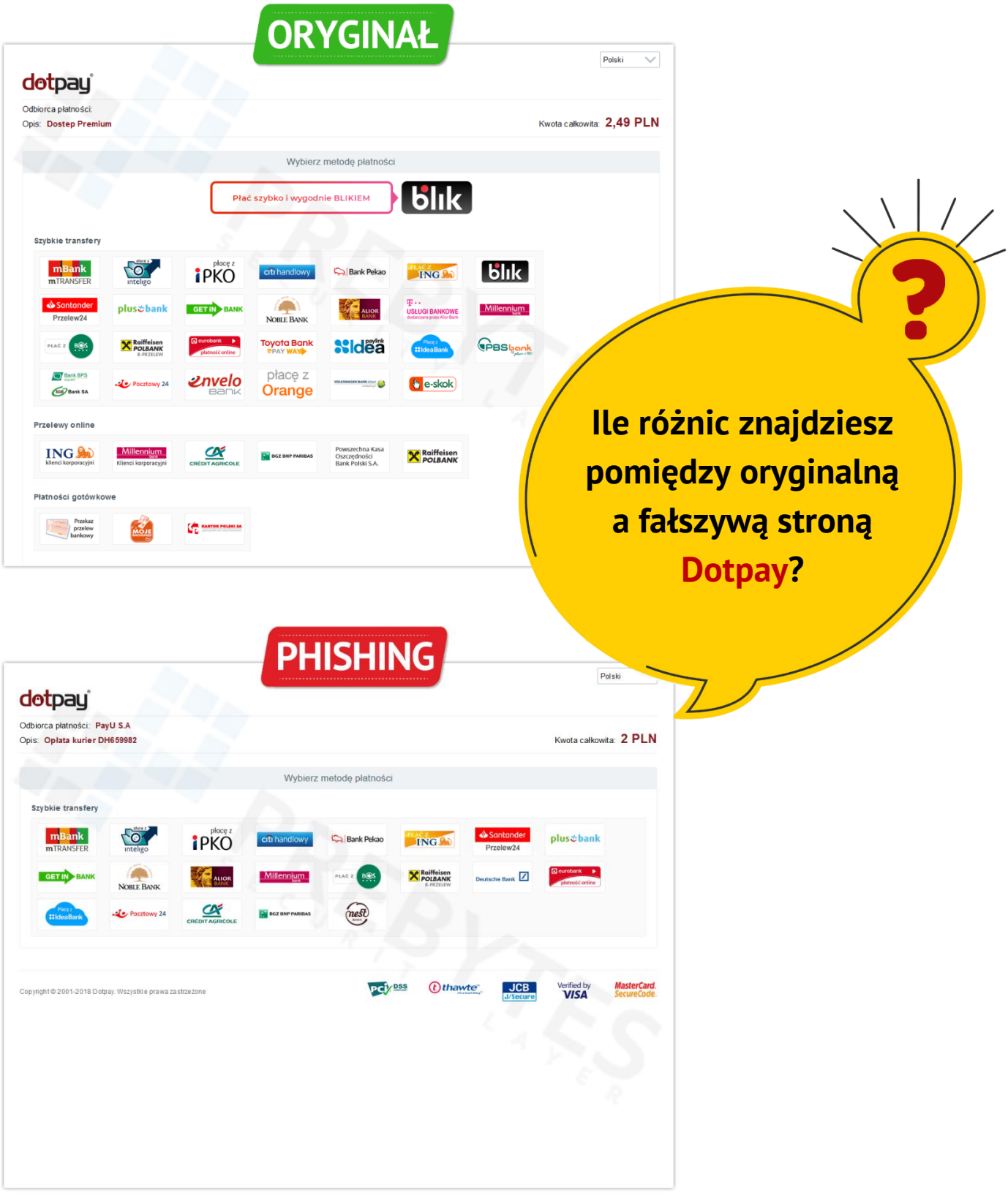


Po wybraniu bankowości na fałszywej stronie szybkich płatności następowało przekierowanie do fałszywej strony banku. Cyberprzestępcy wyłudzali w ten sposób dane autoryzacyjne do bankowości, a następnie kradli pieniądze z konta ofiary.

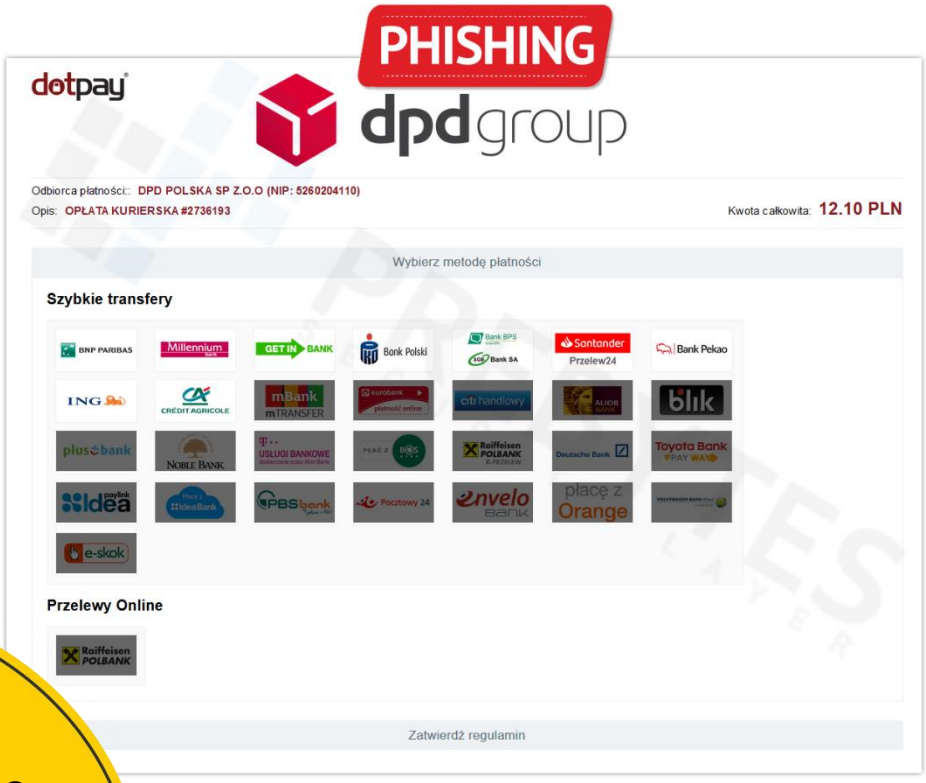
FAŁSZYWE STRONY SZYBKICH PŁATNOŚCI

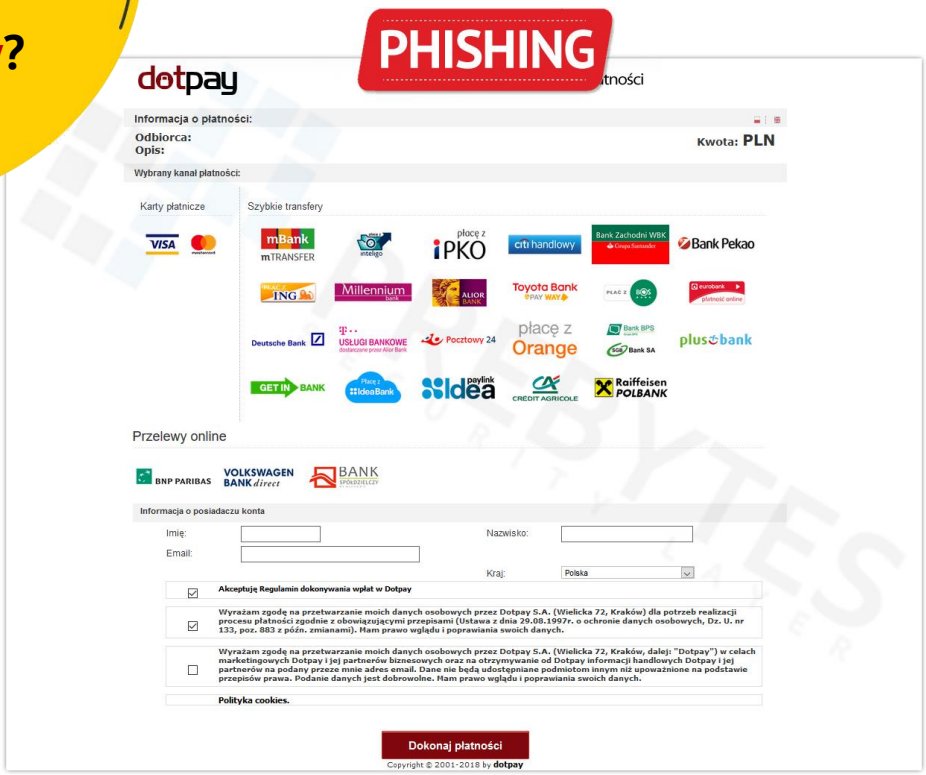
Dotpay

Przestępcy najczęściej fałszowali oryginalną stronę Dotpay. Czasem fałszywa strona Dotpay różniła się od oryginalnej liczbą dostępnych platform bankowości.



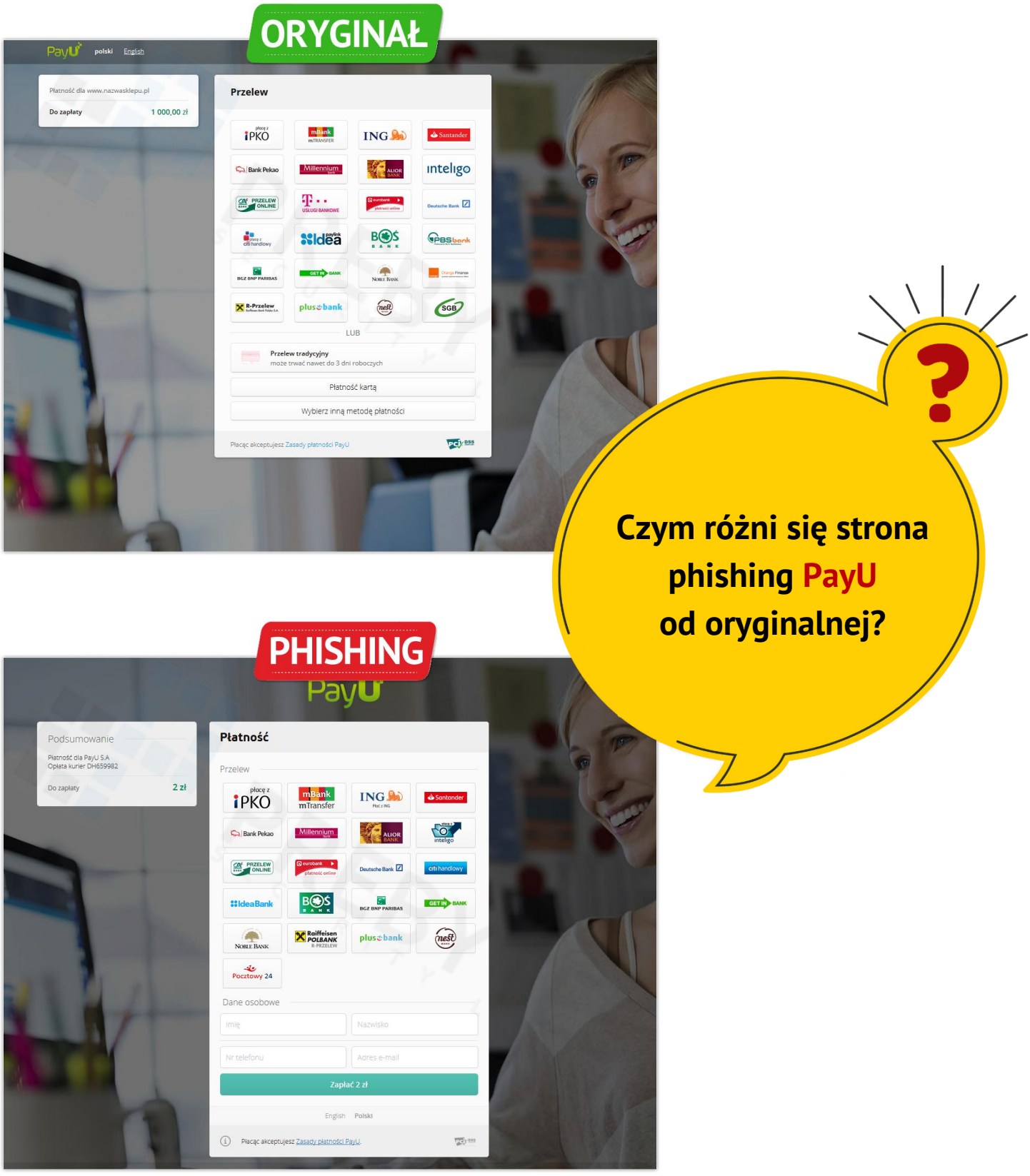
Czy logo Twojego banku znajduje się na fałszywych stronach Dotpay?





PayU

Phishing PayU przygotowany przez przestępców oferował mniej opcji płatności. Dodatkowo nie wspierał tradycyjnego przelewu oraz płatności kartą.



Przelewy24

Fałszywa strona podszywająca się pod Przelewy24 oferowała zdecydowanie mniejszą liczbę dostępnych form płatności. Umieszczono na niej również opcję blik - choć była ona nieaktywna.

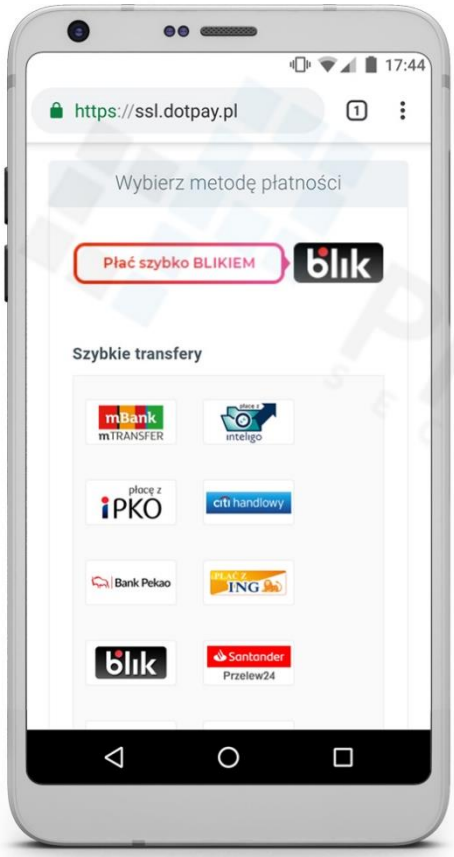


PHISHING NA URZĄDZENIACH MOBILNYCH

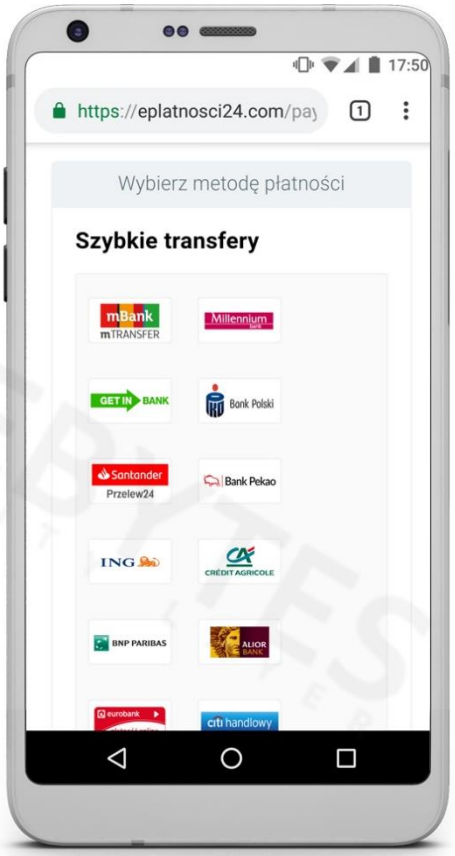
Przestępcy w atakach phishing często wykorzystywali wiadomości SMS wysyłane do potencjalnych ofiar. Umieszczali w nich link do fałszywej strony płatności. Ofiara klikając w link była przekierowywana do strony, której autentyczność była jeszcze trudniejsza do oceny.

Aktualnie przeglądarki mobilne nie wyświetlają rozszerzonych certyfikatów SSL EV, które uwiarygadniają oryginalne strony polskich banków, Dotpay, PayU i platformy Przelewy24. Certyfikaty SSL EV symbolizowane są w tym przypadku jedynie przez zieloną kłódkę. W przeglądarkach desktopowych obok zielonej kłódki możemy zobaczyć również nazwę organizacji, do której należy certyfikat.

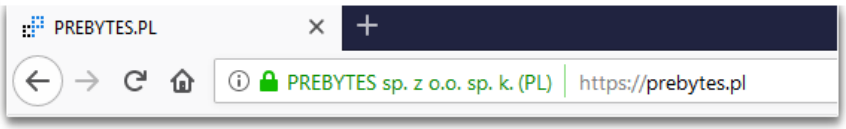
Oryginalna strona Dotpay



Fałszywa strona Dotpay



Certyfikat SSL EV



Charakterystyczną cechą tego certyfikatu jest wyświetlanie nazwy organizacji obok zielonej kłódki w pasku adresu. Żadna z przeglądarek mobilnych nie wyświetla certyfikatu SSL EV.

Dowiedz się więcej na ten temat czytając nasz artykuł:

https://sirt.pl/certyfikaty-w-przegladarkach-mobilnych/

PAMIĘTAJ!



Na stronach szybkich płatności oraz stronie Twojego banku zawsze sprawdzaj, czy nazwa domeny jest poprawna oraz, czy strona posiada certyfikat SSL EV.

Szczególną ostrożność zachowaj podczas korzystania z bankowości na urządzeniach mobilnych. Jeśli nie jesteś pewien autentyczności strony płatności i nie wiesz w jaki sposób to sprawdzić – lepiej ją opuść.





Dodaj bezpłatny dodatek **BrowserWall** do swojej przeglądarki! Jeśli nieświadomy zagrożenia będziesz próbował wejść na stronę phishing – **BrowserWall** zablokuje Ci do niej dostęp i tym samym ochroni Cię przed utratą pieniędzy.

Jeśli otrzymasz link do płatności w wiadomości email, SMS-ie bądź na portalu społecznościowym - nie klikaj w niego, to może być oszustwo. Natychmiast zgłoś to na **zglosincydent.pl**!



PREBYTES

tel: +48 17 785 19 85
fax: +48 17 240 21 43
hello@prebytes.pl

ul. Sandomierska 6
37 – 300 Leżajsk



https://prebytes.pl/



https://sirt.pl/



https://www.facebook.com/PREBYTES.SIRT/



https://twitter.com/PREBYTES_SIRT/



https://zglosincydent.pl/



https://browserwall.com/

Copyright © 2019 Prebytes. All rights reserved.

Wszelkie informacje w tym dokumencie mogą ulec zmianie bez uprzedniej informacji oraz są przedstawione na zasadach „TAKIE JAKIE JEST" (AS IS).

PREBYTES nie udziela absolutnie żadnych gwarancji – całościowych lub/oraz częściowych na wszystkie informacje tekstowe, obrazkowe oraz binarne. PREBYTES dokłada wszelkich starań, aby dane zawarte w raporcie były kompletne, aktualne i zgodne ze stanem faktycznym, nie może tego jednak zagwarantować i w związku z tym faktem nie ponosi żadnej odpowiedzialności za skutki wykorzystywania prezentowanych danych, w szczególności za szkody powstałe w wyniku korzystania z nich. W żadnym wypadku PREBYTES nie ponosi odpowiedzialności za wszelkie skutki lub szkody, w tym bezpośrednie, pośrednie, przypadkowe, wynikowe, utratę zysków handlowych lub szkody specjalne, wynikające z lub w związku z używaniem lub rozpowszechnianiem informacji zawartych w niniejszym raporcie.

Zabronione jest wykorzystywanie niniejszego raportu do świadczenia usług naruszających prawa PREBYTES, o ile zawarta umowa nie stanowi inaczej. Dystrybucja niniejszego dokumentu wymaga pisemnej zgody PREBYTES.

Wszelkie zarejestrowane i niezarejestrowane znaki towarowe użyte w tym dokumencie są własnością ich właścicieli.