Najpopularniejsze błędy i metody ataków na aplikacje bankowe

Rafał Gołębiowski
Senior Security Officer, Bank BGŻ BNP Paribas S.A.

BGŻ BNP PARIBAS

Agenda

1. #whoami
2. Najpopularniejsze wektory ataków na bankowość
3. Zagrożenia - Aplikacje Webowe
4. Zagrożenia - Aplikacje Mobilne
5. Przykładowe Ataki na Aplikacje Mobilne
6. Przykładowe Ataki typu Phishing
7. Przykładowe Ataki na Aplikacje WWW
8. Rekomendacje
9. Podsumowanie
10. Pytania?
11. Kontakt

whoami

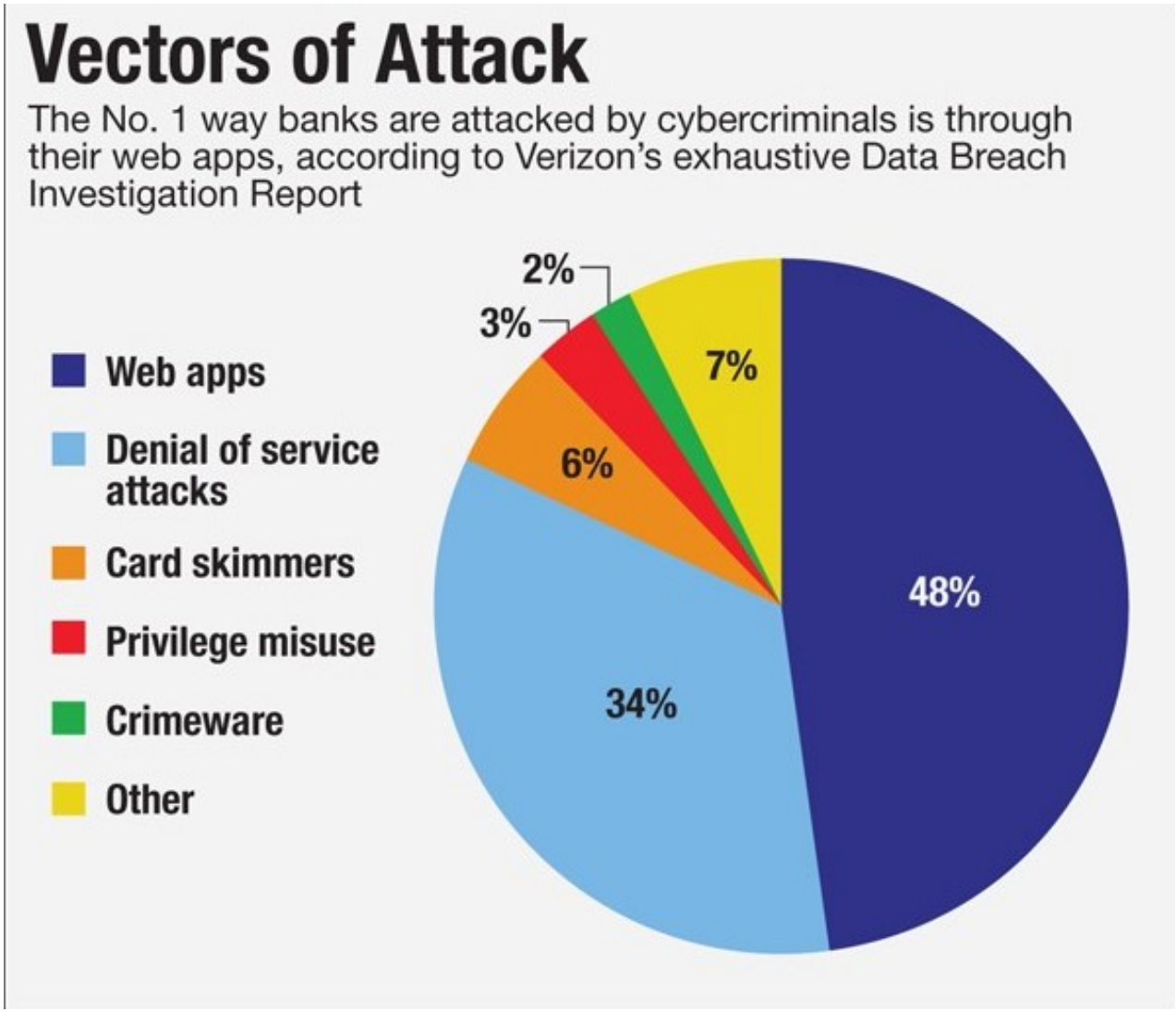
whoami

- **Doświadczenie**
  - Firma wytwarzająca AV na urządzenia mobilne, firma wytwarzająca oprogramowanie, firma konsultingowa, bank

- **Konferencje w ktorych bralem udzial:**
  - SecureTech Congress
  - GigaCon Network Security Congress
  - GigaCon Internet Banking Security
  - IT Security Trends
  - GigaCon Systems Security & Reliableness
  - inne

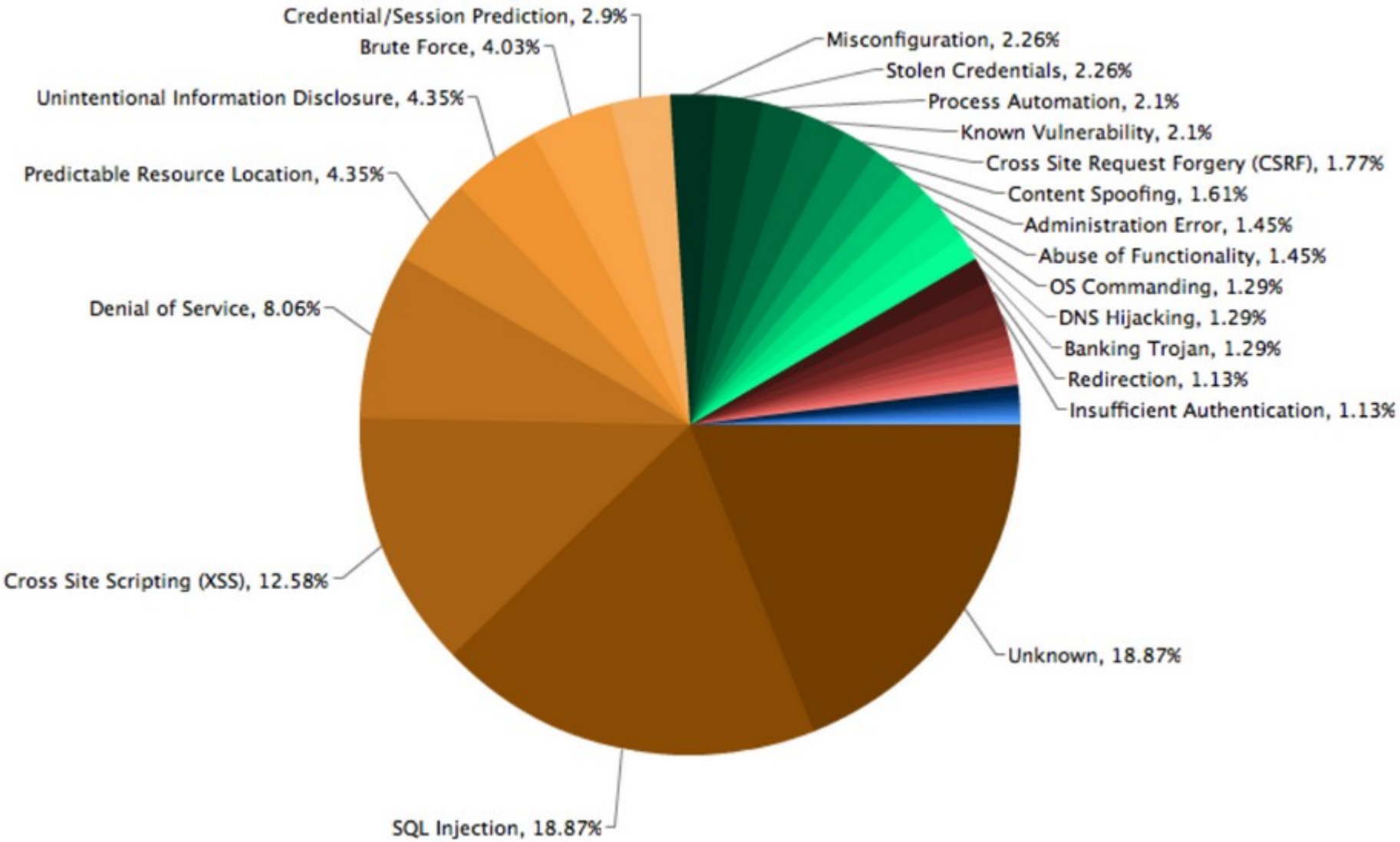
Najpopularniejsze wektory ataków na bankowość

Najpopularniejsze wektory ataków na bankowość



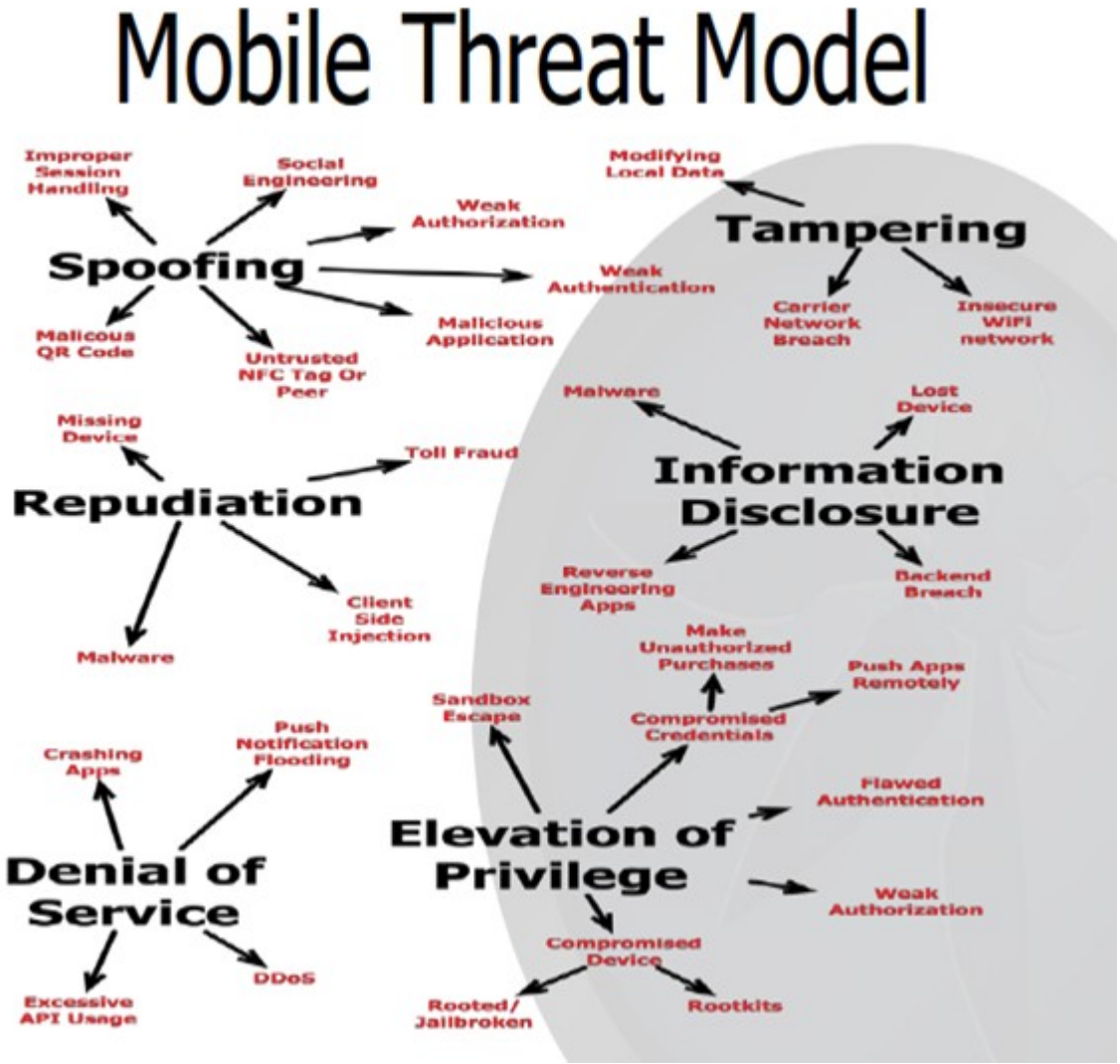
Zagrożenia - Aplikacje Webowe

Aplikacje webowe



Zagrożenia - Aplikacje Mobilne

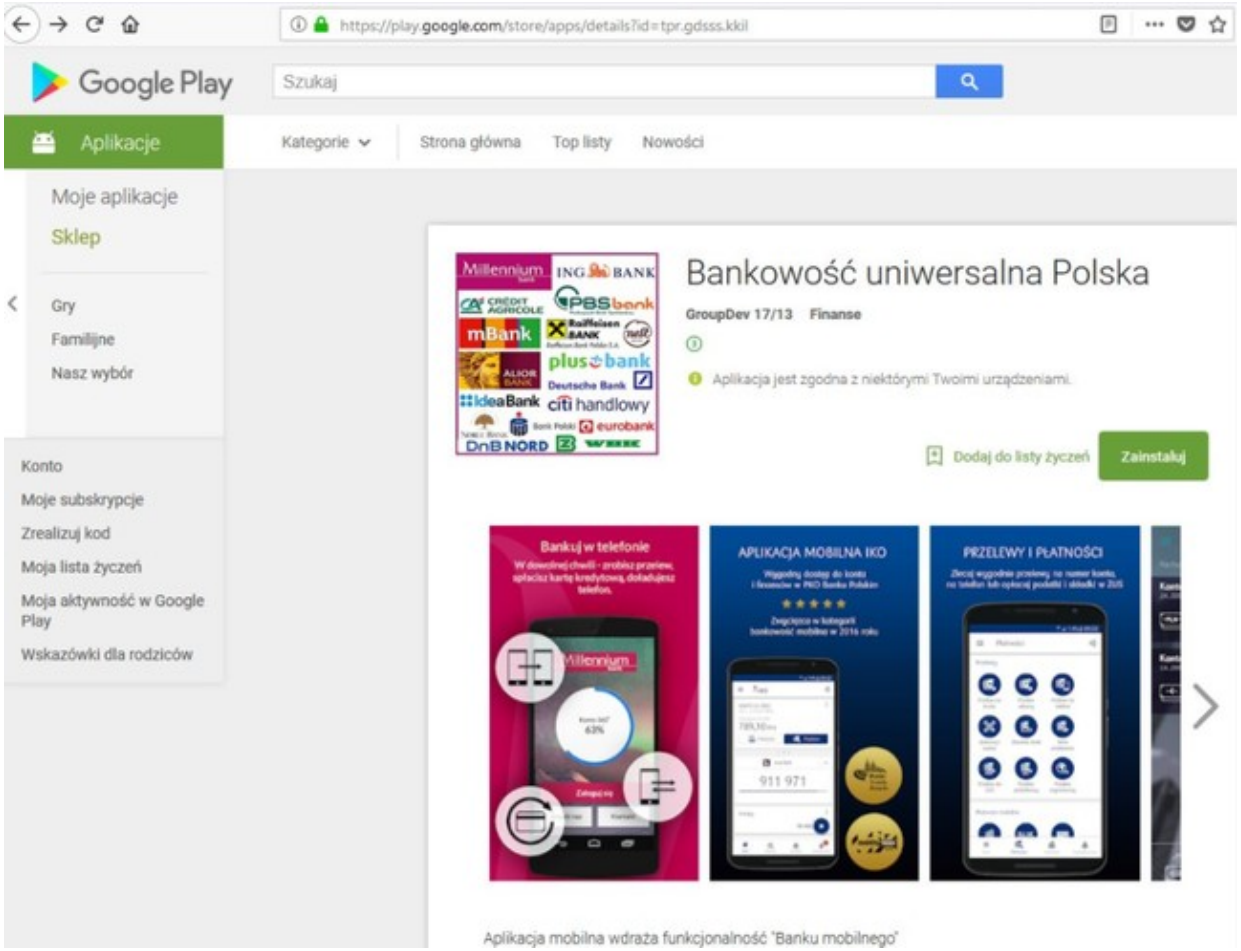
Aplikacje mobilne



Przykładowe Ataki na Aplikacje Mobilne

Aplikacje mobilne

Wyłudzanie poświadczeń poprzez specjalnie dedykowaną aplikację



Aplikacje mobilne

Kompromitacja bankowości mobilnej poprzez “aktualizację systemu operacyjnego”

Program przeszukuje telefon i sprawdza, czy użytkownik korzysta z bankowości mobilnej. W bazie szkodnika zapisanych jest 68 banków, pod które może się podszyć.

W momencie, gdy użytkownik uruchamia aplikację banku, wirus wyświetla okno z prośbą o podanie loginu i hasła. Okno to wyświetla się nad uruchomioną aplikacją banku, powodując jej przysłonięcie. W efekcie wygląda to tak, jakby aplikacja bankowa żądała informacji.

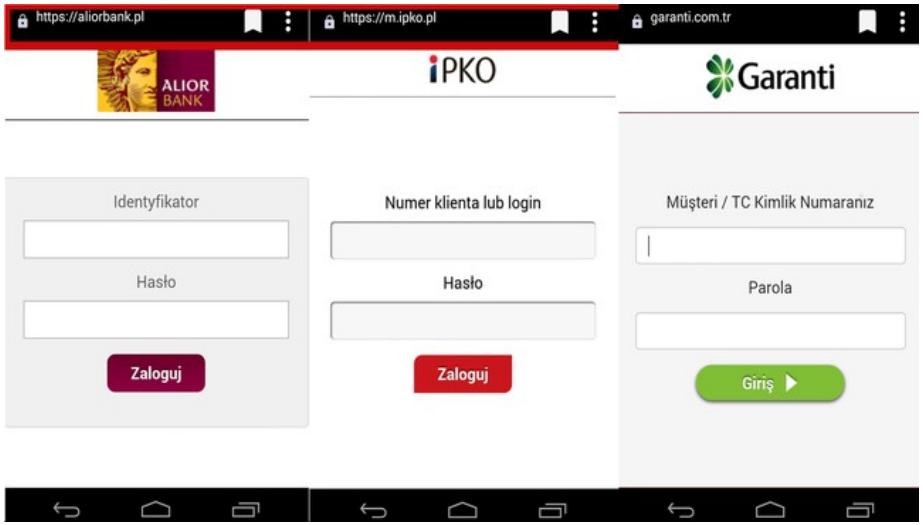
- Wirus jest w stanie przechwytywać komunikaty SMS z kodami autoryzacyjnymi.
- Program wyłudza również numery kart płatniczych poprzez generowanie specjalnych komunikatów proszących o podanie wrażliwych informacji.
- ZBP zwraca uwagę na jeszcze jedną nietypową funkcję wirusa: program potrafi poprosić użytkownika, by zrobił sobie zdjęcie twarzy wraz z widocznym dokumentem tożsamości. Prawdopodobnie dane te zostaną później wykorzystane do otwierania kont w różnych serwisach.

Aplikacje mobilne

Malware GMBot

GMBot rozprowadzany jest głównie poprzez fałszywe strony służące do oglądania filmików. Najczęściej podszywa się pod aktualizację programu Adobe Flash Player lub aplikację PornTube.

Podczas instalacji prosi o nadanie praw administratora, aby móc monitorować otwierane aplikacje oraz łączyć się z siecią WiFi. Po wgraniu jej na telefon aplikacja zaczyna monitorować aktywne procesy.



GMBot potrafi:

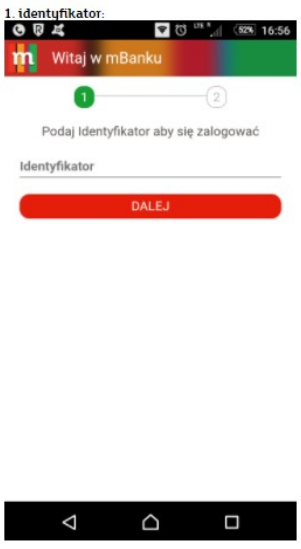
- Przekierowywać połączenie i SMS-y przychodzące na inny numer
- Wykradać dane karty kredytowej z Google Play
- Wysyłać pełną historię przeglądarki na serwer zarządzający
- Przesyłać listę wszystkich aplikacji zainstalowanych na telefonie
- Przesyłać wszystkie SMS-y na serwer zarządzający
- Wysyłać SMS-y do ofiary, aby zachęcić do zalogowania się na konto bankowe

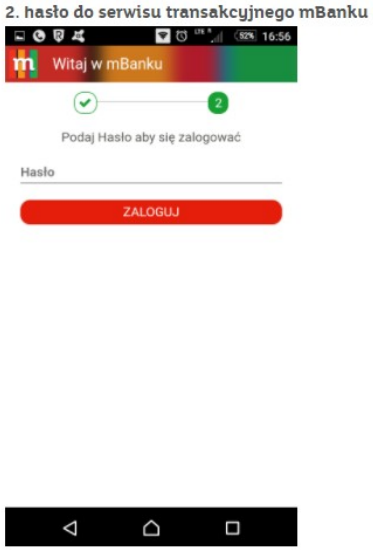
Aplikacje mobilne

“Nakładka” na aplikacje mobilną

Wirus atakuje smartfony z systemem operacyjnym Android. Można paść jej ofiarą nawet po zainstalowaniu aplikacji z oficjalnego sklepu Google. Obecnie wirus podszywa się na przykład pod jedną z aplikacji do sprawdzania kursu kryptowalut.

Po jej pobraniu na zainfekowanym telefonie i włączeniu aplikacji mobilnych kilku polskich banków, można zobaczyć „nakładkę”, podszywająca się pod właściwą aplikację bankową.





Możliwości wirusa

- Przejęcie kontroli nad urządzeniem
- Wykonywanie i podsłuchiwanie połączeń telefonicznych
- Wysyłanie i odbieranie SMSów

Przykładowe Ataki typu Phishing

Phishing

Dostałeś takiego SMS-a? Chcą Cię okraść!

PKO Bank Polski ostrzega przed kolejnym sprytnym przekrętem. Oszuści, podszywając się pod operatorów telefonii komórkowej, informują za pomocą SMS-ów o konieczności spłaty zadłużenia. Podają link, pod którym znajduje się narzędzie do wyłudzania danych.

To kolejna próba wyłudzenia pieniędzy za pomocą rozsyłanych losowo wiadomości SMS. Jak podaje bank, niektórzy klienci mogli otrzymać wiadomość z informacją, że zalegają drobną kwotę, np. 6 zł. Nadawcy ostrzegają, że nieuregulowanie zaległości będzie skutkowało zablokowaniem połączeń telefonicznych. W treści znajduje się link kierujący do sfałszowanej strony internetowej. Link ma być rzekomo aktywny tylko przez 2 godziny.

W ten sposób oszuści poganiają klienta, by szybko zalogował się na stronie i uregulował zaległość. Żądają drobnej kwoty, by uśpić czujność ofiary, bowiem większe stawki wzbudziłyby podejrzenia.

Po kliknięciu w link użytkownik trafia na stronę internetową wyglądającą tak, jak klasyczna bramka płatnicza. Oczywiście nie zgadza się adres, ale nie każdy zwróci na to uwagę.

Po wybraniu swojego banku ofiara zostanie przekierowana do kolejnej fałszywej strony – tym razem wyglądającej jak strona banku. Zostanie tam poproszony o wpisanie loginu i hasła.

Phishing

Fałszywe wiadomości o zablokowanym koncie

---------- Wiadomość przekazana dalej --
Od: **System iPKO** <agata.szymkow80@auder-morasha.edu.pl>
Data: 6 kwietnia 2016 19:53
Temat: Wazna wiadomosc PKOBP
Do:

Data: 06.04.2016 r.

Dostęp do Twojego konta iPKO został zablokowany!

W trosce o bezpieczeństwo naszych klientów zablokowaliśmy konto w systemie iPKO, powodem jest nieautoryzowany dostęp do konta.
W celu odzyskania dostępu prosimy o weryfikację właściciela rachunku, logując się na:

www.ipko.pl

Serdecznie pozdrawiamy,
Zespół PKO Bank Polski

W przypadku jakichkolwiek pytań prosimy o kontakt z Infolinia 801 307 307

Tak wygląda fałszywy e-mail (PKO BP)

W mailu pojawia się link, który kieruje na stronę, imitującą stronę banku.

Na pozór link wygląda identycznie, jak ten prawdziwy.

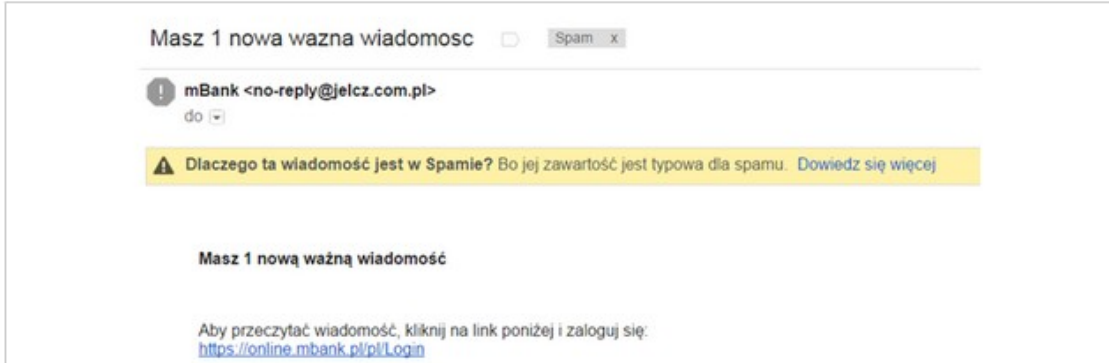
Jednak po jego kliknięciu, nie zgadza się adres strony internetowej.

Podejrzenia powinna zbudzić tez domena, z której wysyłana jest fałszywa wiadomość

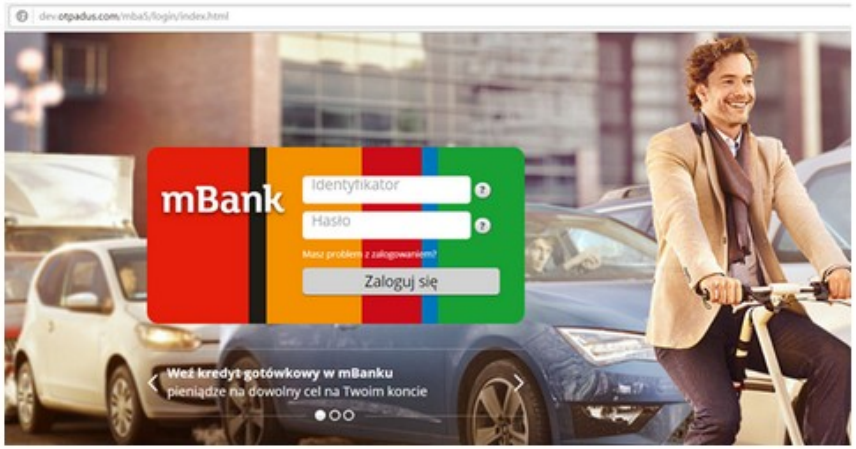
Celem jest wyłudzenie danych

Phishing

Pilne zalogowanie do systemu transakcyjnego



Tak wygląda fałszywy e-mail (mBank)



W informacji podany jest link, który kieruje na fałszywą stronę banku.

Jest ona niemal identyczna jak oryginał, ale różni się ważnym szczegółem: nie zgadza się adres strony internetowej.

Nie zgadza się także domena z której wysłano fałszywą wiadomość.

Po wejściu na stronę klient proszony jest o wpisanie loginu i hasła do bankowości internetowej.

Jeśli je poda, dane te trafią w ręce złodziei, którzy będą mogli wejść na konto i przygotować przelew zewnętrzny.

Przykładowe Ataki na Aplikacje WWW

Ataki na aplikacje WWW

Zablokowano stronę internetową Banku Rosji

Strona internetowa Banku Rosji padła w piątek ofiarą ataku hakerów – podaje „The Wall Street Journal" powołując się na oficjalny komunikat prasowy rosyjskiego banku centralnego.

„Obecnie strona Banku Rosji przeżywa trudności spowodowane atakiem hakerów. Bank Rosji podejmuje działania mające na celu odparcie ataku i przywrócenie jej normalnego funkcjonowania" – poinformowało biuro prasowe rosyjskiego banku centralnego.

O godzinie 10:20 strona Banku Rosji nadal była niedostępna. Dziś Bank Rosji ma podjąć decyzję w sprawie poziomu stóp procentowych. Analitycy zakładają, że główna stawka pozostanie bez zmian na poziomie 7,0%.

Ataki na aplikacje WWW

Kto odpowiada za włamanie na konto? Bank przegrywa w sądzie

“Pieniądze przechowywane na rachunku bankowym przechodzą na własność banku, a wyłudzenie tych środków nie powinno oznaczać, że szkodę poniesie posiadacz konta”

Złodziej przejął kontrolę nad rachunkiem

Zgodnie z ustaleniami sądu do wyprowadzenia pieniędzy z rachunku doszło przy użyciu zarówno bankowości internetowej, jak i telefonicznej. Wszystko odbyło się w ciągu około 20 minut. Sekwencja zdarzeń była następująca:

- nieznany sprawca próbował, bez powodzenia, trzykrotnie zmienić hasło w bankowości internetowej. Dostęp do serwisu transakcyjnego został zablokowany.
- Nieznany sprawca zalogował się do serwisu bankowości telefonicznej (podając numer klienta i telekod) i ustalił nowe hasło do bankowości internetowej.
- Złodziej połączył się z infolinią banku, zalogował się i podając się za posiadacza rachunku zlecił pracownikowi dokonanie zmiany numeru telefonu, na który przesyłane są hasła jednorazowe SMS.
- Pracownik infolinii zweryfikował dane podawane przez połączoną osobę, uzyskał poprawne odpowiedzi i ręcznie zaktualizował numer telefonu.
- Nieznany sprawca zalogował się do serwisu bankowości internetowej i zlecił przelew na ponad 120 tys. zł.

Prawowita posiadaczka rachunku otrzymała SMS z informacją o dokonanej zmianie numeru telefonu. Wiadomość odczytała jednak dopiero wieczorem i zlekceważyła powiadomienie jako „błąd systemu”.

Rekomendacje

Rekomendacje

- ✓ Zgodność z OWASP Top10 (OWASP ASVS) dla aplikacji WWW
- ✓ Zgodność z OWASP Mobile
- ✓ Periodyczne testy penetracyjne
- ✓ Prowadzenie kampanii uświadamiającej użytkowników
- ✓ Monitorowanie tzw *Threat Landscape*
- ✓ *Inne*

OWASP
Open Web Application Security Project

OWASP
Mobile Security Project

RECOMMENDED

Podsumowanie

Podsumowanie

- Lwia część udanych ataków na pieniądze klientów banków pocchodzi bezpośrednio lub pośrednio przez phishing
- Bezpieczeństwo środków bankowych to odpowiedzialność zarówno banku jak i właścicieli środków
- Bank był, jest i będzie zawsze atrakcyjnym celem dla hakerów
- Bank wdrażając systemy bezpieczeństwa, które ograniczają wygodę użytkowników robią to dla ich dobra (np. Wymuszanie zmiany hasła)
- Każdy upubliczniony udany atak na bankowość to cios w reputację banku, bez względu na to czy wina leżała po stronie klienta czy banku

Pytania?

Pytania?

Kontakt