



U mnie (nie)działa. Prawie wszystko, co chcesz wiedzieć o monitorowaniu aplikacji, ale nie masz kogo zapytać.

Mateusz Ossowski - [Monit24.pl](https://monit24.pl)

ROZKŁAD JAZDY

3 IX 2023
11 XI 2023

PRZYJAZDY

GOŁOZ PRZYJAZDY	STACJA POCHODZENIA	PRZEZ	PRZEZ	KODZ. POCHAGU	KODZ. POCHAGU	OPÓŹN. min	PERON
13.06	LUBLIN AIRPORT		SWIDNIK MIASTO	REGIO			2
13.09	SZASTARKA		KRASNIK	REGIO			2
13.12	WARSZAWA Wsch.	LUKOW	LUBARTOW	REGIO			1
13.16	DEBLIN	PULAWY M.	NALECZOW	REGIO			3
13.21	CHELM	REJOWEC	SWIDNIK MIASTO	REGIO			2
13.28	BYDGOSZCZ GŁOWNA	KUTNO	DEBLIN	REGIO			2
14.14	CHELM	REJOWEC	SWIDNIK MIASTO	REGIO			1
14.28	ZAMOSC Wschod.	REJOWEC	SWIDNIK MIASTO	REGIO			1b
15.12	TERESPOL	DEBLIN	NALECZOW	REGIO			1a
15.25	CHELM	REJOWEC	SWIDNIK MIASTO	REGIO			1

WIFI

1) kursy 12-13:00 1. XI;
2) kursy 13:00-14:00 2. XI;
3) kursy 14:00-15:00 3. XI;
4) kursy 15:00-16:00 4. XI;
5) kursy 16:00-17:00 5. XI

14) kursy 14:00-15:00 1. XI;
15) kursy 15:00-16:00 2. XI;
16) kursy 16:00-17:00 3. XI;
17) kursy 17:00-18:00 4. XI;
18) kursy 18:00-19:00 5. XI

Rozkład jazdy

#1 Intro

- Cele na dziś
- Dlaczego monitoring jest jak cebula?
- Co robi McGyver w Monit24.pl ?
- Żółw wodny
- Wyjście przez sklep z pamiątkami.

#2 Podsumowanie

- Checklista
- Q&A

#1 Intro

Moje prawdziwe cele

1

Chciałbym pokazać, holistyczne podejście do monitoringu i gdzie my w tym jesteśmy.

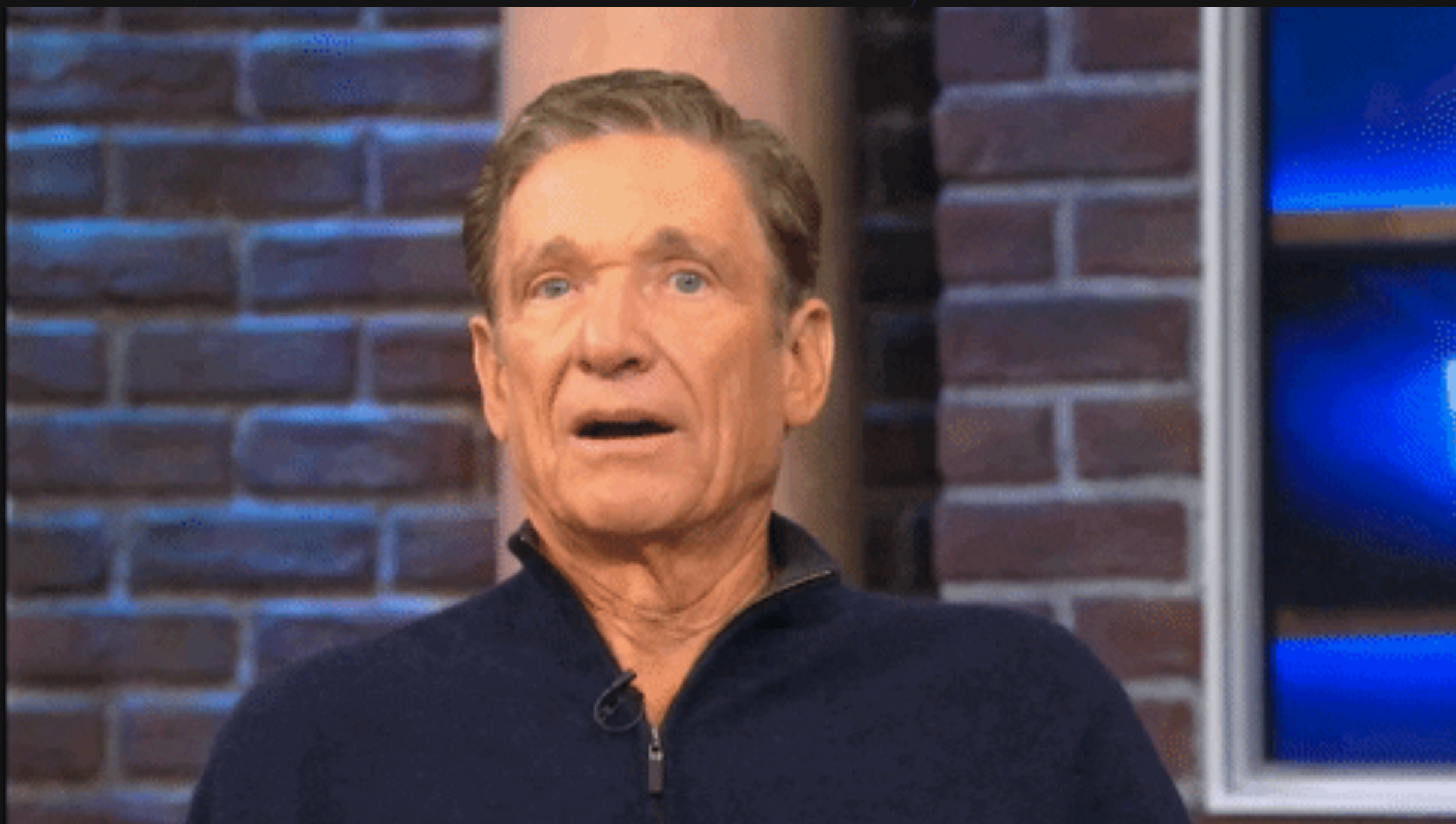
2

Wiecie jakie, są problemy techniczne, kiedy budujecie monitoring skomplikowanego procesu a nie samego kodu! Będziecie wiedzieć, które z nich możecie rozwiązać sami, a które outsourcować. **Co robić, a czego nie robić w domu?**

3

Pokazać nieoczywiste kierunki eskalacji błędów.

WIEM CZEGO SIĘ BOICIE



Mateusz Ossowski

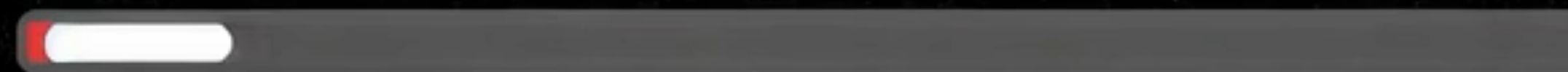
Channel **Sales** Director

509 746 430

mateusz.ossowski@monit24.pl

Czy znasz to uczucie ?

N



LOADING...





#eskalacja
#inne działy
#Jira

Warstwy monitoringu systemów IT

1. Sprzęt / Infrastruktura

CPU, RAM, dyski, interfejsy sieciowe, zasilanie

2. System operacyjny

procesy, usługi, uptime, load, logi systemowe

3. Usługi / Middleware

bazy danych, kolejki, serwery aplikacyjne, cache, połączenia

4. Aplikacje



API, mikroserwisy, logika biznesowa, błędy, czasy odpowiedzi

5. Doświadczenie użytkownika



testy syntetyczne, transakcje, dostępność, RUM

6. Biznes / KPI



SLA, SLO, koszty przestoju, wskaźniki biznesowe

Odtwarzamy konkretne działania w twojej aplikacji.



Przejęcie pełnej ścieżki zakupowej, wraz z wyszukiwaniem produktu, dodaniem do koszyka, zalogowaniem się, wybraniem metody dostawy, przejściem do bramki płatności.



Monitorowanie serwisów WWW i natywnych aplikacji mobilnej, odtwarzanie zaplanowanych procesów biznesowych.



Badanie działania API.



Testy wydajnościowe dla podstron lub całych procesów.



Odtwarzanie dowolnych scenariuszy z wieloma metodami autoryzacji, jak: kody SMS, autoryzacja mobilna, tokeny sprzętowe, certyfikaty i pozostałe.

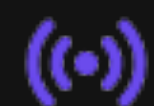


Sprawdzanie działania formularzy ofertowych, kalkulatorów składek itp.



Monitorowanie strumienia video, wyświetlania się reklam, działania platform wymiany walut wraz z ciągłą analizą strumienia danych (np. aktualność notowań).

Cechy systemu Monit24



Monitorowanie 24h ze 150 lokalizacji.



Możliwość integracji i automatyzacji (pełne API w oparciu o OpenAPI).



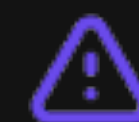
Szczegółowe powiadomienia dla techników, raporty okresowe dla kierownictwa i organów nadzorczych (np. Spełnienie SLA, compliance).



Dashboard z aktualnym stanem badanych usług.



Panel z dostępem on-line przez przeglądarkę WWW i aplikację mobilną.



Powiadomienia o wystąpieniu awarii przez wybrane kanały, również bezpośrednio do systemów IT klienta, eskalacje.



Nagrania video z każdego sprawdzenia, screenshot, HAR i inne artefakty przesyłane w powiadomieniu o zdarzeniu.



Własne laboratorium z fizycznymi telefonami do odtwarzania scenariuszy na mobile.

Pozostałe cechy systemu Monit24



Model SaaS – brak potrzeby instalowania aplikacji i ingerencji w infrastrukturę klienta.



Zapis ładowania się strony i wszystkich jej elementów na każdym kroku scenariusza (HAR).



Możliwość monitorowania wielu typów usług np. działania API, poczty elektronicznej, DNS, systemów bazodanowych, tras routingu, poprawności SSL, OCSP i innych usług w oparciu o protokół IP.



Powiadomienia o awariach (SMS, PUSH, e-mail, Slack, MS Teams, Signal i inne), raporty okresowe SLA (na email w PDF).



Zapis zawartości strony WWW, screen i wideo z momentu wykrycia awarii + istotne informacje diagnostyczne



Możliwość dostosowania raportów i funkcjonalności systemu do specyficznych wymagań Klienta.

JA MAM
MONITORING

ALE NIE ODTWARZASZ
TESTU NA PRODUKCJI



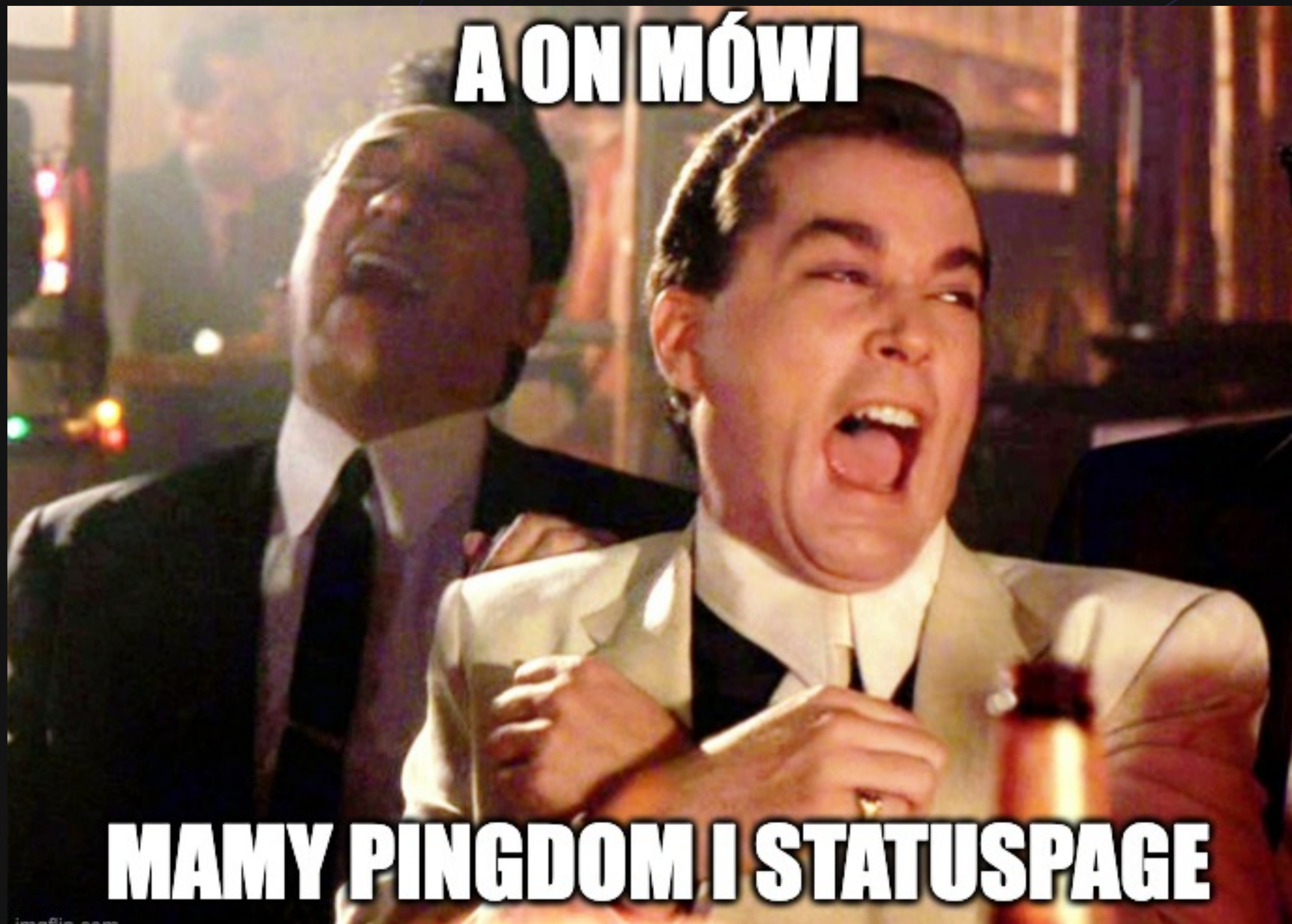
Serwer - Czy działa ?

Backend/API - Czy spełnia warunki

Serwis www - Czy nie zamula ?

Użytkownik w aplikacji web/mobile - Czy może wykonać proces biznesowy ?

Dlaczego monitoring jest taki ważny ?



Dlaczego monitoring jest taki ważny ?



Dlaczego monitoring jest taki ważny ?

Going.app

Start przedsprzedaży

Tango down web+mobile (Ddos+boty zakupowe)

Dlaczego monitoring jest taki ważny ?

Going.app

Start przedsprzedaży

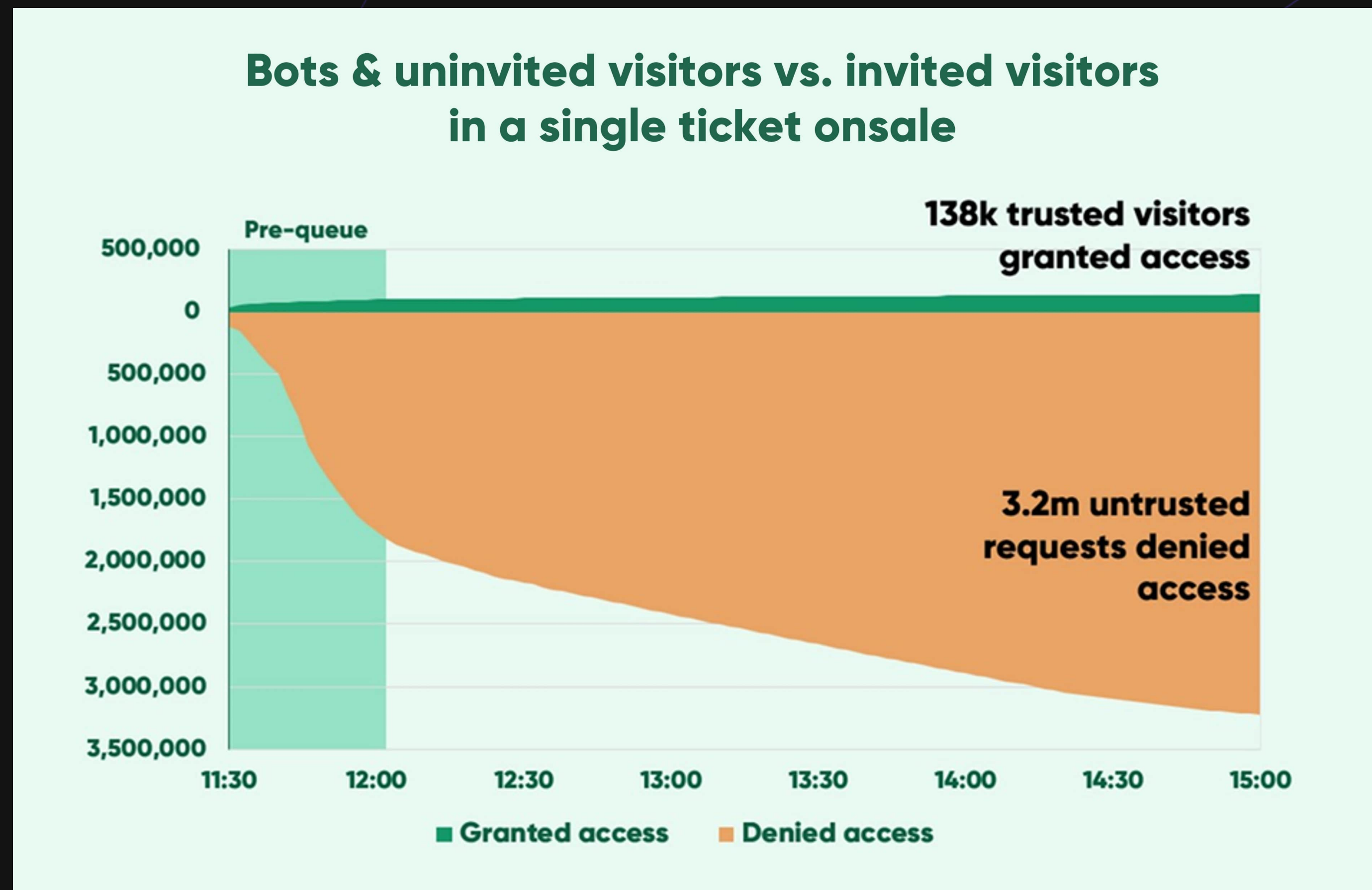
Tango down web+mobile (Ddos+boty zakupowe,

Przesunięcie na godz. 12

Kolejny „ostatni” koncert - efekt Najmana

Voucher na 25 zł jako rekompensata :)

Queue.it - boty to 40% ruchu - zadanie dla WAFa



Queue.it - boty to 40% ruchu - zadanie dla WAFa

Queue.it

How ticket bots snatch tickets

Account
creation



Account
takeover



Simulating
many users



Speedy
scripted bots



Credit
card fraud



Purchases
exceeding limits



1. Prior to onsale

2. During onsale wait

3. During ticket purchase

Ticket Scalping

WAF, Captcha, Fingerprinting, ML, wIDS,

Taylor Swift, Key Investment Group, 49 kont, 274 bilety (limit 6 na osobę, McGyver), 119 000 \$.

<https://www.reuters.com/sustainability/boards-policy-regulation/us-ftc-sues-ticket-reseller-evading-taylor-swifts-eras-tour-ticket-limits-2025-08-18/>

<https://datadome.co/learning-center/how-to-stop-online-bot-ticket-scalping-and-other-ticketing-industry-bot-threats/>

FIND AN NATB MEMBER

Use this tool to find a Member of The National Association of Ticket Brokers.

Close

About

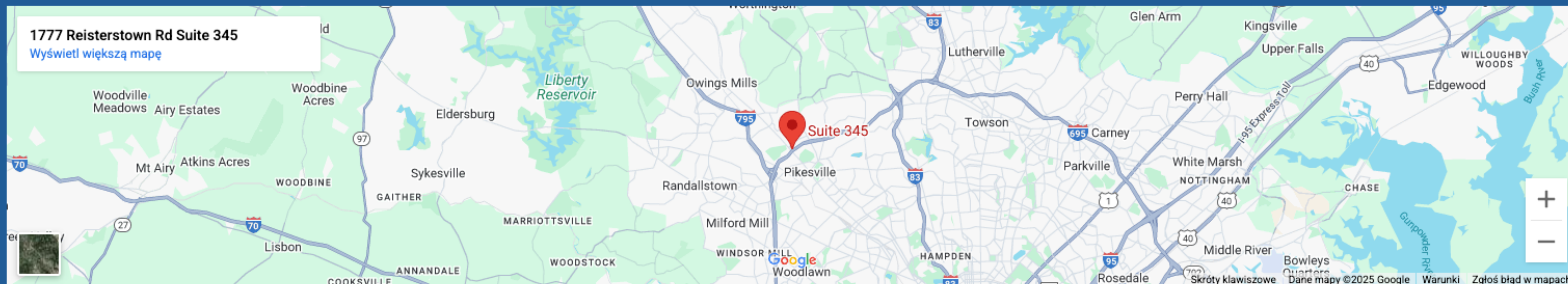
✕ Post

🔄 Share

Key Investment Group, LLC

1777 Reisterstown Rd Suite 345

[Wyświetl większą mapę](#)



Key Investment Group, LLC

📍 1777 Reisterstown Rd Suite 345
Pikesville MD 21208, US

☎ [917-576-6090](tel:917-576-6090)

✉ [Send a Message](#)



Rynek botów ticketowych

fiverr.🔍Fiverr ProExploreEnglishBecome a SellerTry Fiverr GoSign inJoin

Graphics & DesignProgramming & TechDigital MarketingVideo & AnimationWriting & TranslationMusic & AudioBusinessFinanceAI ServicesPersonal Growth

Get the best ticket bot services

Find the best ticket bot services you need to help you successfully meet your project planning goals and deadline

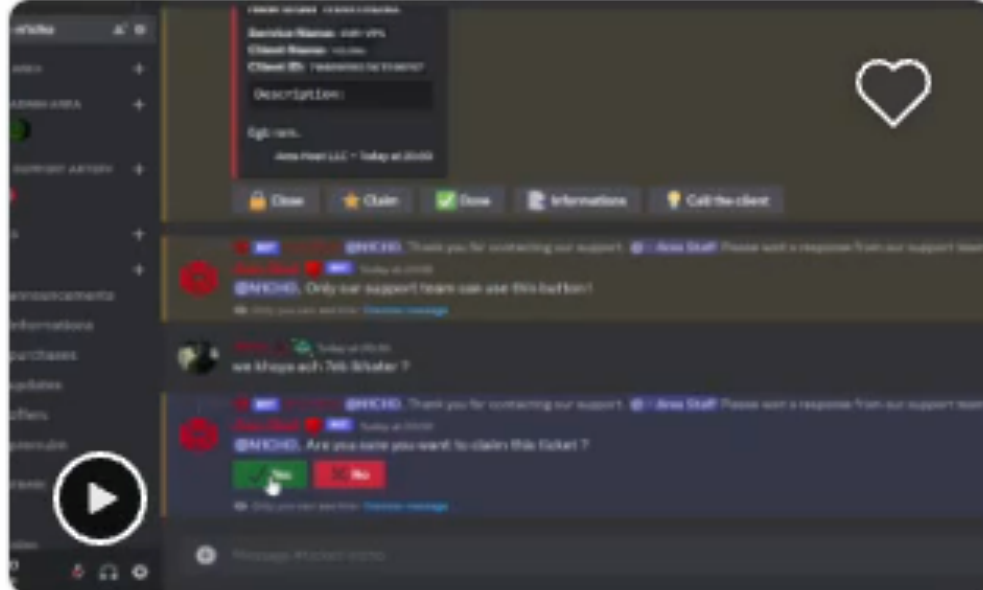
[Join Fiverr](#)

2088 services available



Expert C
I will develop ticketing bot, ticketmster, chelsea, queue it

From \$100



Rayyane
I will create a custom ai discord ticket bot for you

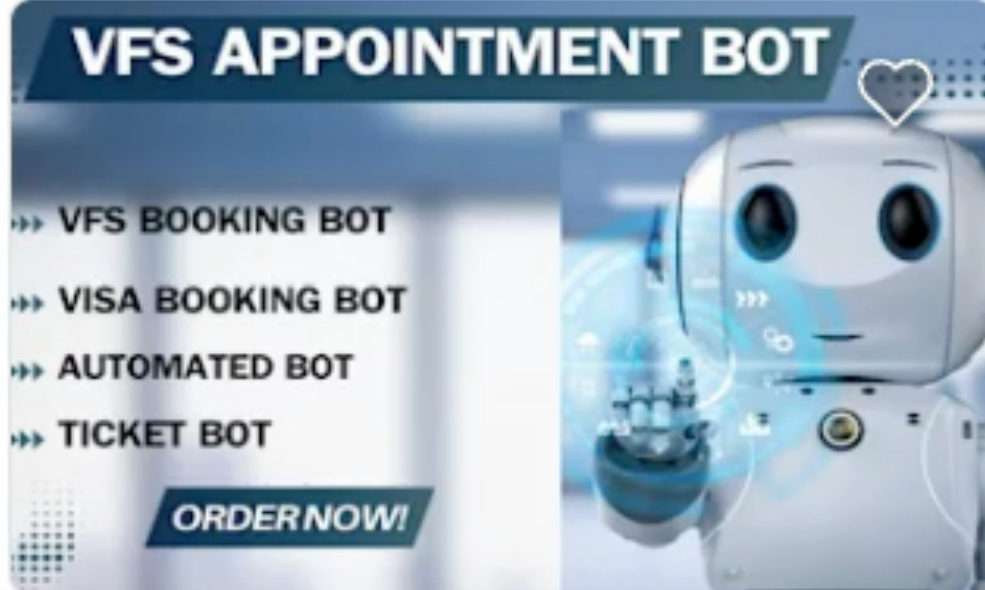
★ 4.8 (23)

From \$30



Sarah R
I will setup shoes bot, snkrs app bot, kobe shoes bot, snkrs bot, tinder...

From \$100



Duane M
I will setup shoes bot, snkrs app bot, kobe shoes bot, snkrs bot, tinder...

From \$100

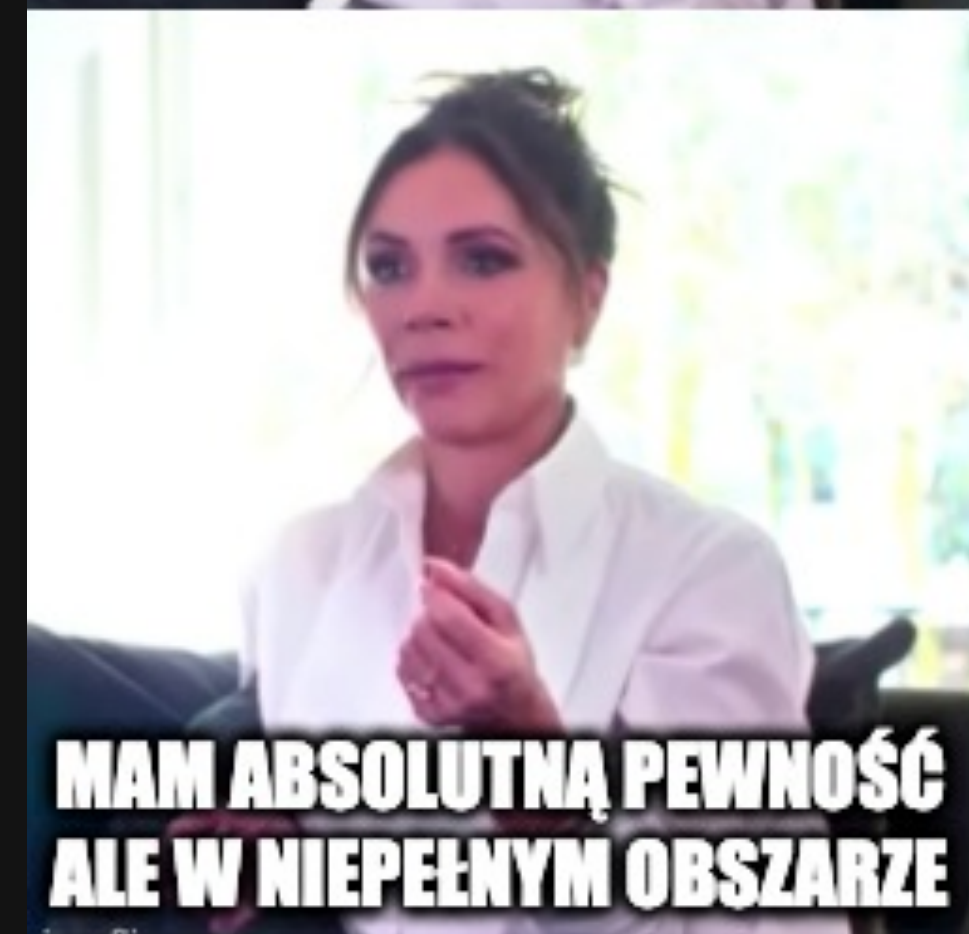
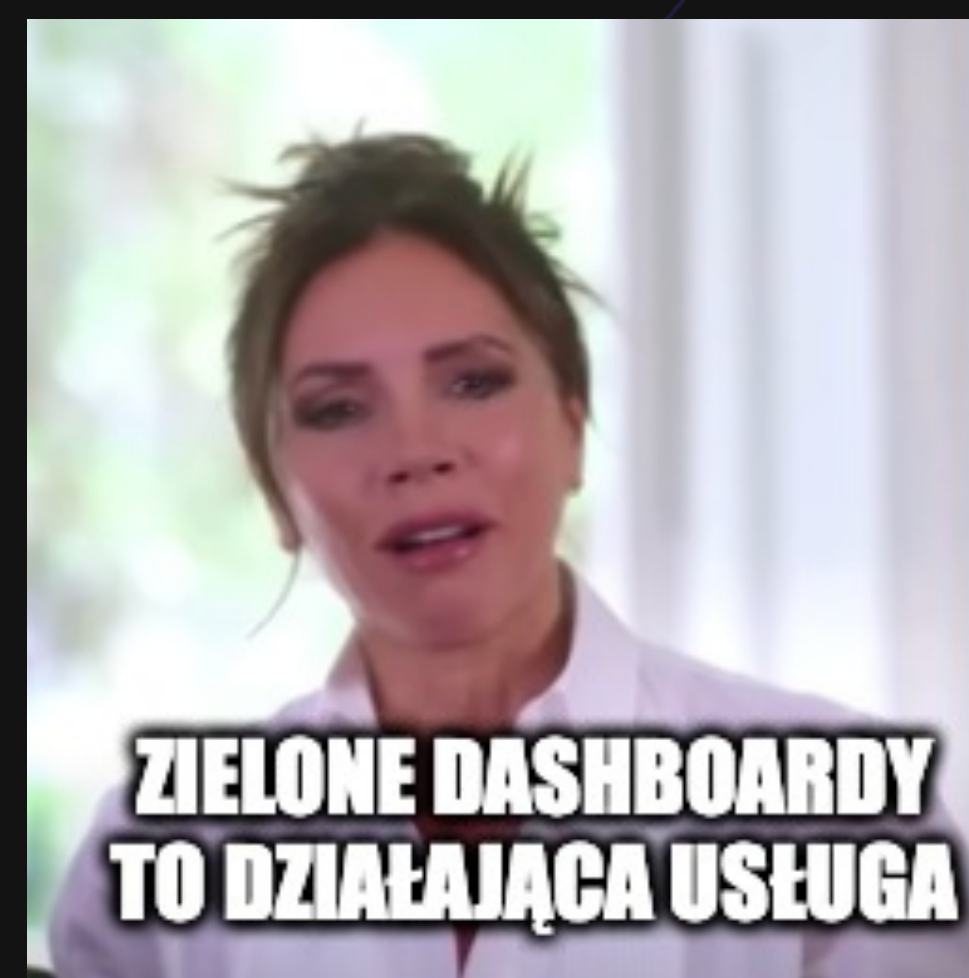
DIY ticket bot

<https://medium.com/@benlahner/how-to-build-your-own-ticket-bot-63c3d0706e92>

<https://github.com/topics/ticket-bot>

Konik wiecznie żywy :)

WAF+test wydajnościowy



Case Study - Ecommerce

Dla naszego klienta Rossmann realizujemy m.in. test zakupu obejmujący zweryfikowanie czy prawidłowo załadowały się wszystkie elementy i certyfikaty. Scenariusz obejmował między innymi:

- wyszukanie produktu
- dodanie produktu do koszyka
- zalogowanie się do konta Rossmann
- wprowadzenie kuponu rabatowego
- wybranie metody dostawy i uzupełnienie adresu
- realizację płatności na bramce
- sprawdzenie odebrania maila z potwierdzeniem realizacji zamówienia



Każdorazowo scenariusz jest realizowany z minimum 3 lokacji i łącz w Polsce.

W związku z tym, że test odbywał się co kilka minut a wybraliśmy najtańszy produkt w sklepie Rossmann był gotowy do wysłania 300 mydełek dziennie.

Odpowiadamy na pytanie, czy klient może dokonać zakupu.

Wdrożenie Monit24 nie wymaga żadnych prac programistycznych po stronie klienta. Wyjątkiem może być udostępnienie VPN lub odpowiedniej reguły dla Web Application Firewalla.

Bezpłatny 30 dniowy okres testowy pozwala na konfigurację kilku scenariuszy klienta. Jeśli wymagana jest personalizacja to w zależności od stopnia skomplikowania może być to jednorazowo płatna konfiguracyjna np. postawienie środowiska w laboratorium dla aplikacji mobilnych. Zobacz przykładową konfigurację tutaj.

Monit24 jest oferowany w formie saas lub on-prem.



Po co sprawdzać od strony usera?



U MNIE NIE DZIAŁA



U MNIE DZIAŁA

To pokaż mi to, ze wszelkimi artefaktami...



- Pulpit
- Monitoring
- Grupy
- Raporty
- Lokacje
- Statusy Zdarzeń
- Zdarzenia
- Kontakty

Szukaj

elementy (16) limit 1 - 16 50

P2

. Monit Panel check
39 minut typ panel_demo kategoria Aplikacje Webowe grupa Demo Services

3-step FullPage scenario !
11 godzin typ Onet kategoria Usługi podstawowe grupa Demo Services

P2

404 TEST
typ FullPage kategoria Usługi podstawowe grupa Demo Services**Auto-paused for maintenance**
typ ping kategoria Usługi podstawowe grupa Demo Services

P2

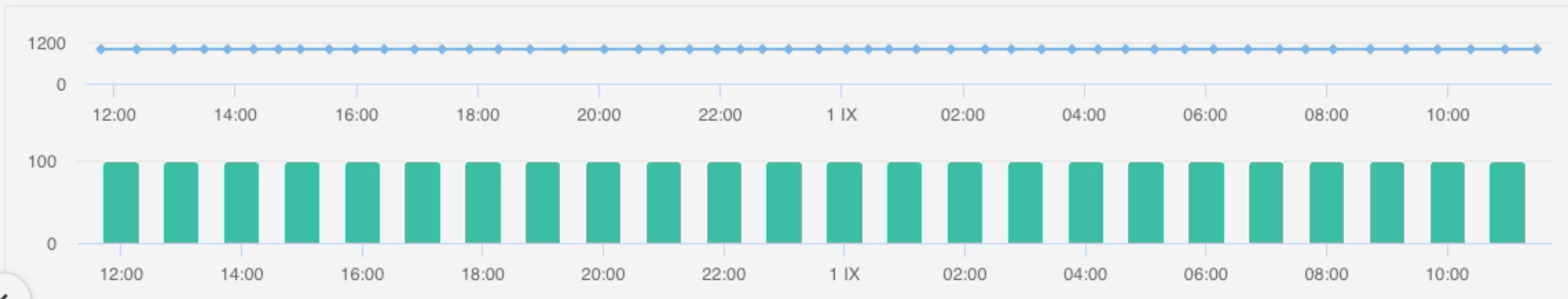
Defence24
12 godzin typ WebAppCheckHttps kategoria Aplikacje Webowe grupa Demo Services**Errors generator :)**
4 minuty typ FullPage kategoria Usługi podstawowe grupa Demo Services**Just ping my web**
typ ping kategoria Usługi podstawowe grupa Demo Services**Meta FilterError**
typ MetaServiceAndGroupMonitor kategoria Usługi podstawowe grupa Demo Services

P4

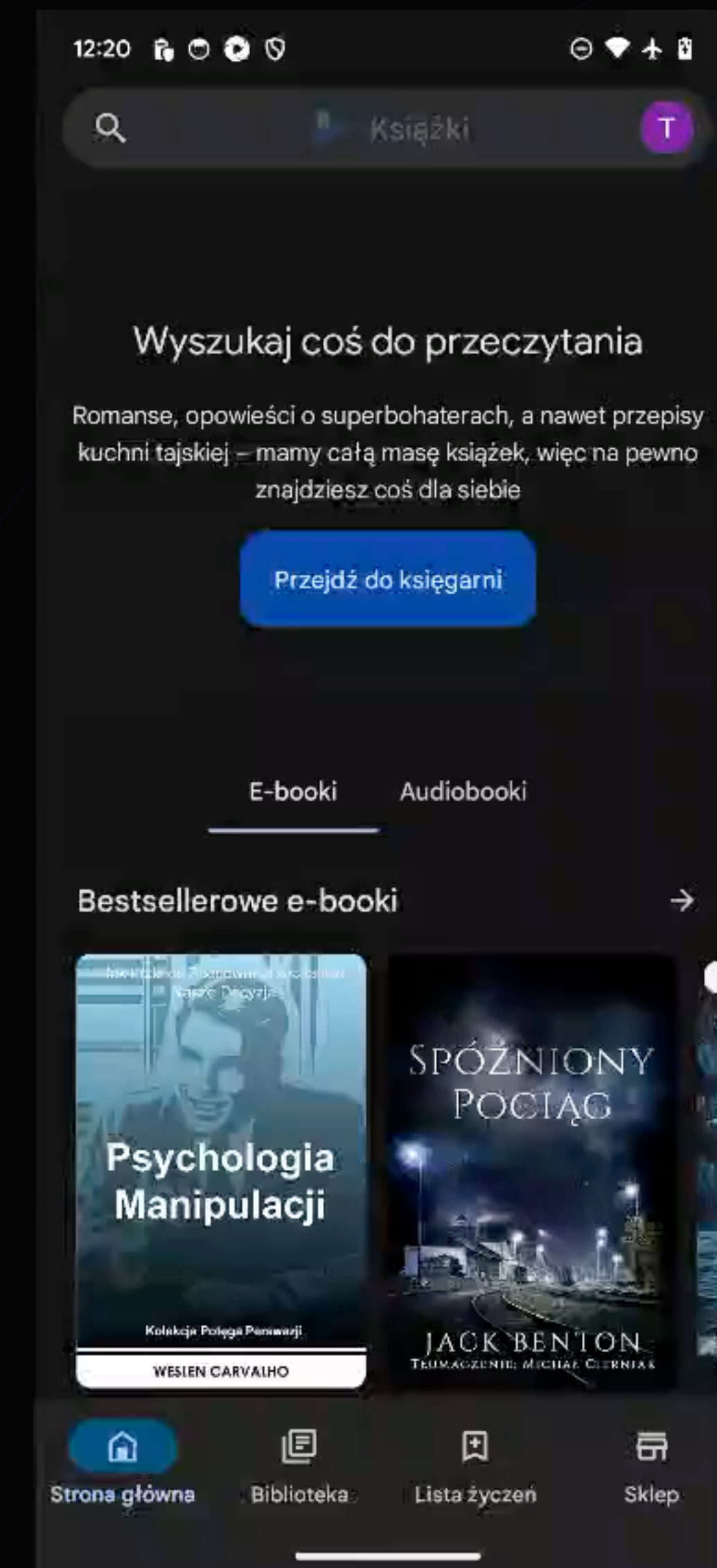
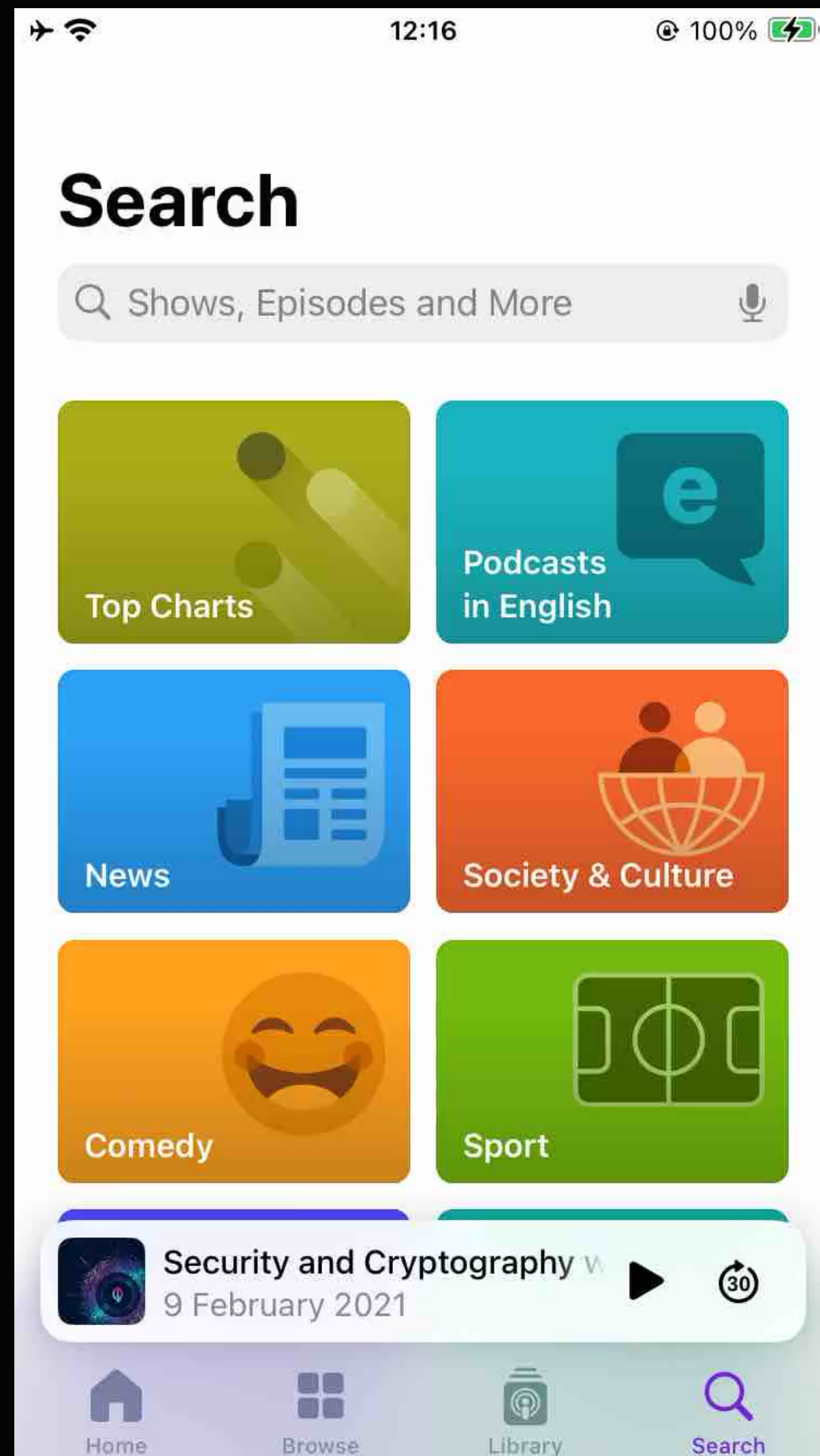
Old admin panel HTTPs check

Wykryte błędy: 1

404 TEST	FullPage
. Monit Panel check	panel_demo
3-step FullPage scenario !	Onet
Defence24	WebAppCheckHttps
Errors generator :)	FullPage
Just ping my web	ping
Meta FilterError	MetaServiceAndGroupMonitor
Old admin panel HTTPs check	https
reply mismatch test check	FullPageHttps
sprint	WebAppCheckHttps
wp.pl news portal FullPage	FullPageHttps
www.monit24.pl via Starlink	FullPageHttps

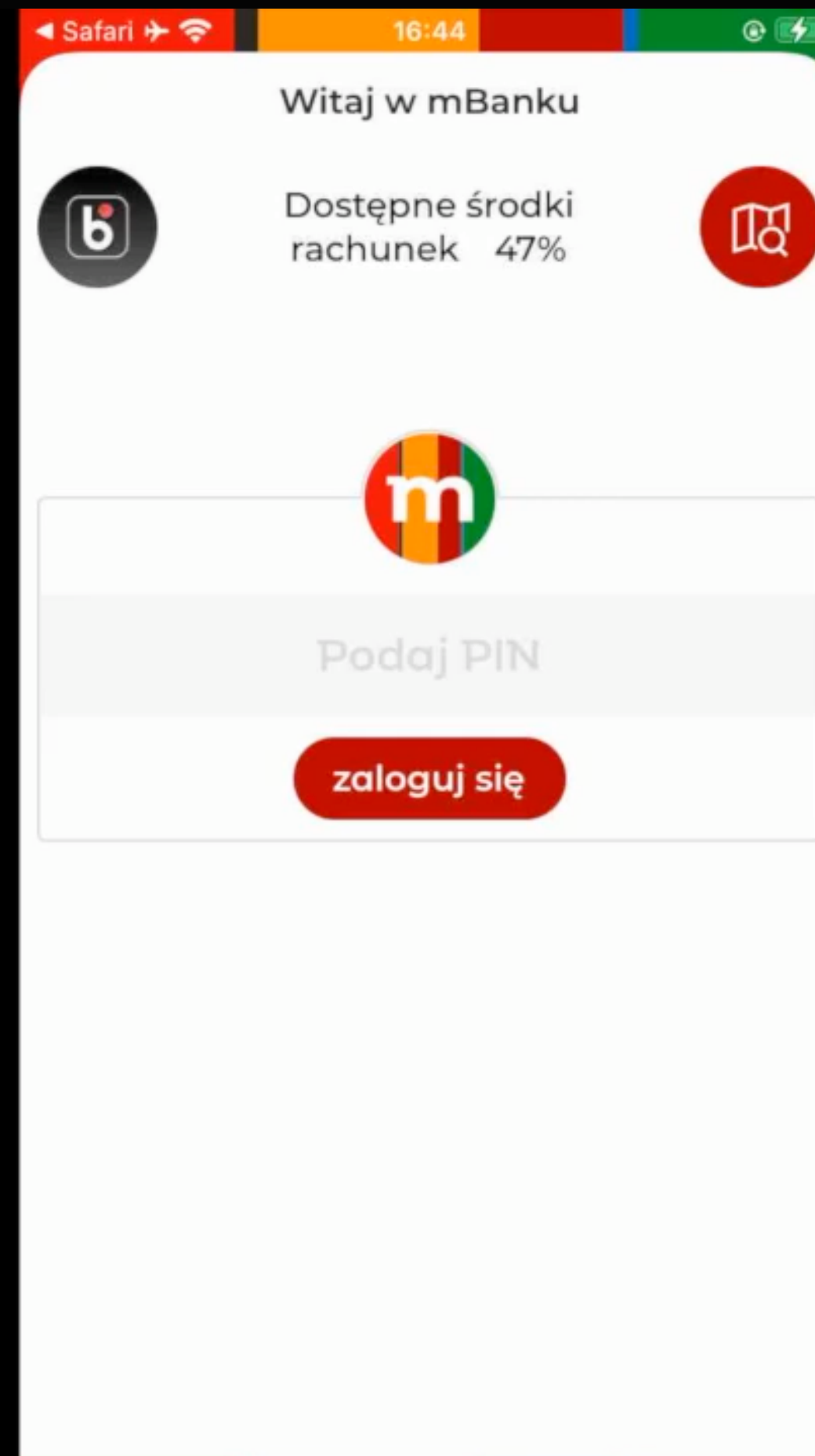


Przykładowy scenariusz mobile iOS/Android



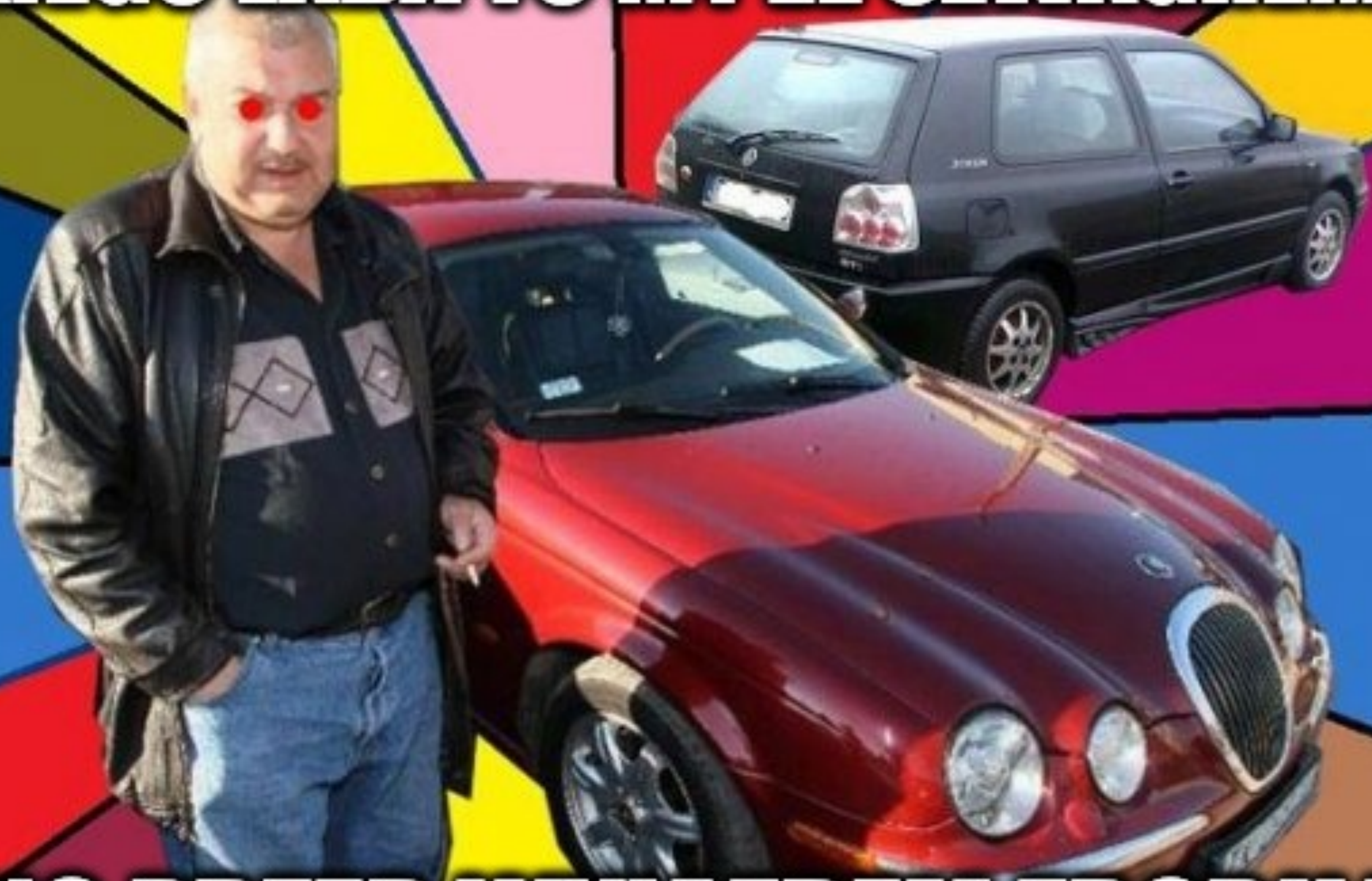
LAB WEB - PSD2 c.d.

Mobile Auth





TAKIEGO LABA TO MY ZE SZWAGREM



RANO PRZED WYJAZDEM ZROBILI

Zaadresowanie błędu - informacje o błędach przychodzą z „góry” a czasami „z zewnątrz”. U MNIE NIE DZIAŁA, U MNIE DZIAŁA.

Eskalacje wewnętrzne

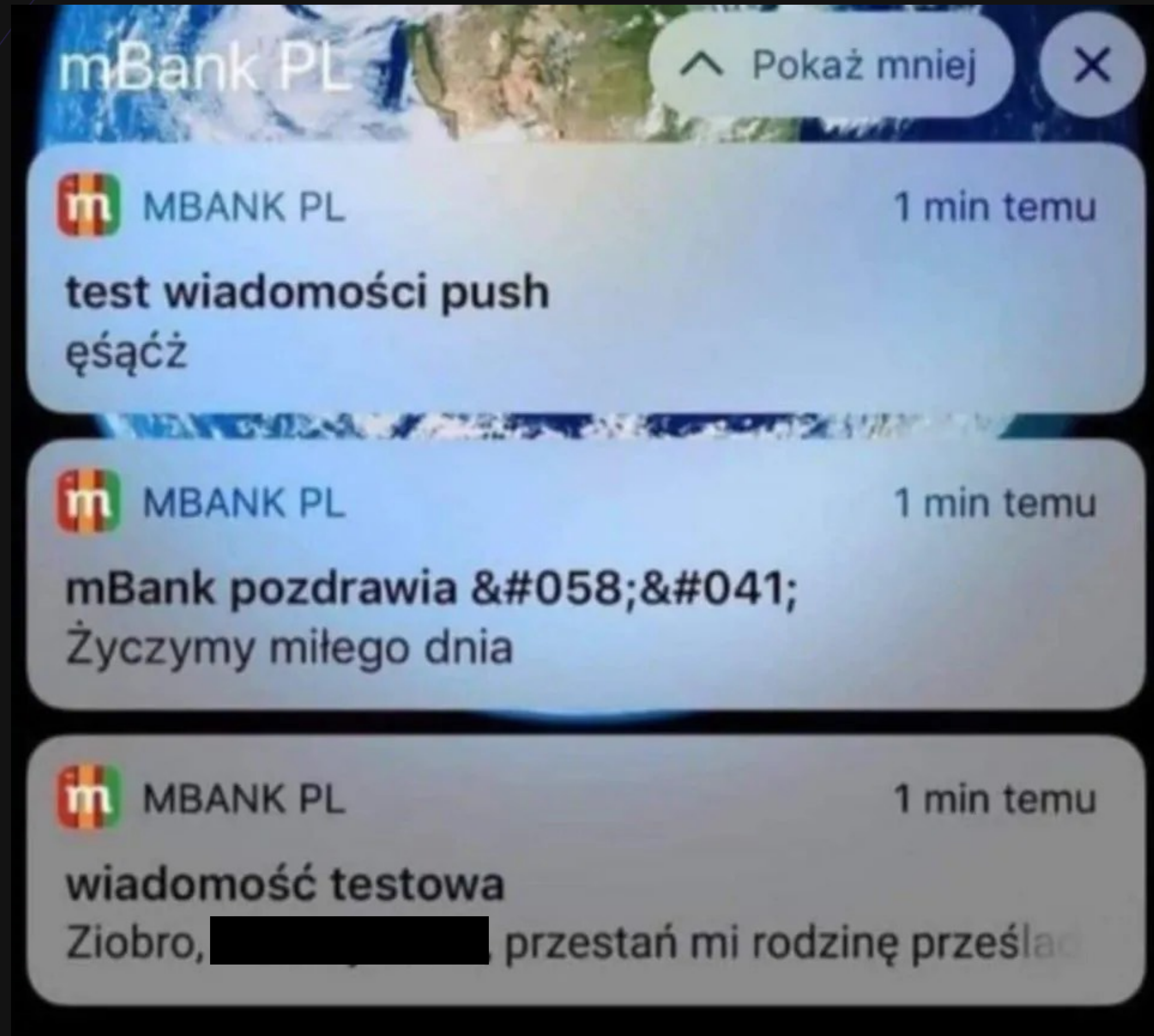
Deeskalacja - gaś ogień zanim będzie pożar.

Monitorowanie od strony przeglądarki/natywnej aplikacji mobilnej.

Skąd te opcje ?

R&D=klienci

np. Testy regresji dla środowisk
UTA/DEV/PRE-PROD



Skąd te opcje ?

R&D=klienci np. Testy regresji dla środowisk UTA/DEV/PRE-PROD

Power care - know how w cenie produktu.

Polska myśl szkoleniowa...

Jesteśmy polskim vendorem i rozumiemy specyfikę naszego rynku.

Przykładowy scenariusz web (Profil Zaufany)



Przykładowy scenariusz web (Profil Zaufany)

The screenshot displays the homepage of the **pacjent.gov.pl** website. The header includes the Polish coat of arms, the website name, and navigation links such as 'Aktualności', 'Internetowe Konto Pacjenta', 'Na ratunek', 'Profilaktyka', 'Załatw sprawę', and 'Systemy zdrowotne'. A 'Zaloguj się' button is highlighted in the top right corner. The main content area features a large blue button labeled 'Zaloguj się na IKP' and two links: 'Jeśli nie masz jeszcze profilu zaufanego, zobacz, jak go założyć' and 'Możesz mieć Internetowe Konto Pacjenta w Twoim telefonie. Zainstaluj mojego IKP, bezpłatną aplikację mobilną'. A 'Virtual assistant' chat window is open on the right, offering help with various services like e-prescriptions and appointments. The footer contains a disclaimer about data processing and a video player interface at the bottom.

pacjent.gov.pl

Serwis Ministerstwa Zdrowia i Narodowego Funduszu Zdrowia

Telefoniczna In...

[Zaloguj się](#)

Unia Europejska

[Aktualności](#) [Internetowe Konto Pacjenta](#) [Na ratunek](#) [Profilaktyka](#) [Załatw sprawę](#) [Systemy zdrowotne](#)

Zaloguj się na Internetowe Konto Pacjenta

[Zaloguj się na IKP](#)

[Jeśli nie masz jeszcze profilu zaufanego, zobacz, jak go założyć](#)

[Możesz mieć Internetowe Konto Pacjenta w Twoim telefonie. Zainstaluj mojego IKP, bezpłatną aplikację mobilną.](#)

Administratorem danych osobowych przetwarzanych na Internetowym Koncie Pacjenta jest Minister Zdrowia. Dane kontaktowe Admin Danych: Ministerstwo Zdrowia, ul. Miodowa 15, 00-952 Warszawa, e-mail: kanclaria@mz.gov.pl. Dane na Internetowym Koncie Pacjer przetwarzane po to, by udostępnić pacjentom informacje o zdarzeniach medycznych, które ich dotyczą. Każdej osobie, której dane są pi przysługuje prawo do: dostępu do danych osobowych, ich sprostowania lub uzupełnienia, ograniczenia przetwarzania, wniesienia skargi nadzorczego. [Pełna informacja o przetwarzaniu danych osobowych](#)

Virtual assistant

Potrzebujesz pomocy związanej z IKP, mojego IKP, e-receptą, e-skierowaniem i innymi e-usługami ochrony zdrowia? Zadać mi pytanie lub wybierz jeden z poniższych tematów:

- Інформація для пацієнтів
- Aplikacja mobilna mojego IKP
- Szczepienie przeciw HPV
- Jak dodać dziecko do IKP
- Szczepienie przeciw COVID-19
- Zdarzenia medyczne

Enter your question here

0:01 / 0:20

Przykładowy scenariusz web (Profil Zaufany)



gov.pl



polski

Zaloguj się do usługi Internetowe Konto Pacjenta

Wybierz bezpieczny sposób logowania

**Profil zaufany**
Użyj loginu i hasła lub bankowości elektronicznej

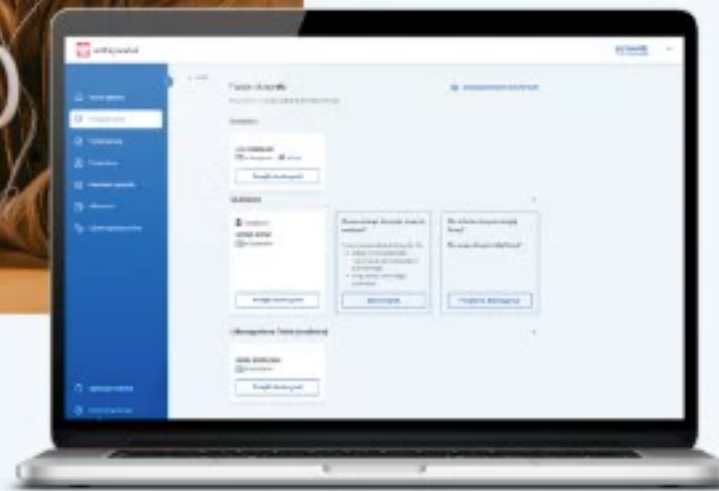
**Aplikacja mObywatel** Polecany
Skanuj kod QR za pomocą aplikacji mObywatel

**Bankowość elektroniczna**
Zaloguj się za pomocą bankowości elektronicznej

**e-Dowód**
Użyj aplikacji mobilnej lub komputera z czytnikiem

**USE eID**
Use your National eID to access online services

**e-Doręczenia**



Załącz skrzynkę e-Doręczeń

odbieraj polecony z urzędu przez Internet

Przejdź do e-Doręczeń

0:03 / 0:20

Monit24

Przykładowy scenariusz web (Profil Zaufany)

Serwis Rzeczypospolitej Polskiej

Login 

Profil zaufany

Zaloguj się za pomocą nazwy użytkownika lub adresu e-mail

[PL](#) | [UA](#)

Nazwa użytkownika lub adres e-mail

[Nie pamiętam nazwy użytkownika](#)

Hasło

[Nie pamiętam hasła](#)

ZALOGUJ SIĘ

LUB

Zaloguj się przy pomocy banku lub innego dostawcy


Bank Polski


mBank


envelo


e-dowód

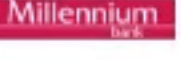

Santander


B.S.

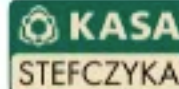

Bank Pekao


VELO


ING


Millennium


ALIOR BANK


KASA STEFCZYKA


CREDIT AGRICOLE


BOŚ BANK


inteligo

0:05 / 0:20

Nie masz profilu zaufanego?



Przykładowy scenariusz web (Profil Zaufany)

[Wysoki kontrast](#) [PL](#) [UA](#)



[JAK KORZYSTAĆ](#) [BEZPIECZEŃSTWO](#) [AKTUALNOŚCI](#) [POMOC](#) [KONTAKT](#)

Błąd

Wewnętrzny błąd serwera.

Identyfikator błędu: 62-250323-030216-0BEF1E

[← Przejdź do strony głównej](#)



[RODO](#) [MAPA STRONY](#)

Portal nadzorowany przez [Minister Cyfryzacji](#). © Wszystkie prawa zastrzeżone.

UWAGA! W trakcie korzystania z profilu zaufanego na komputerze użytkownika przechowywane są informacje (tzw. „ciasteczka”, ang. „cookies”), które pozwalają na dostosowanie świadczonych usług elektronicznych do indywidualnych potrzeb użytkowników. Warunki przechowywania lub dostępu do plików cookie mogą być określone przez użytkownika w ustawieniach przeglądarki internetowej. Kontynuacja korzystania z Profilu Zaufanego bez dokonania wyżej wspomnianych zmian w ustawieniach przeglądarki internetowej uznana zostaje za wyrażenie zgody przez użytkownika na wykorzystywanie plików cookie. Więcej znajdziesz w [Polityce Cookies](#).

▶ 0:06 / 0:20

A teraz coś z zupełnie innej beczki!



DNS - książka telefoniczna internetów
SPF-redirect/impersonate
Chronimy aplikacje, DNSów nie dotykamy bo...

Dorwać się do konta, które ma dostęp do DNS
Modyfikacja i przekierowanie ruchu do infrastruktury
atakującego
Podmiana certyfikatu TLS.

securelist.com

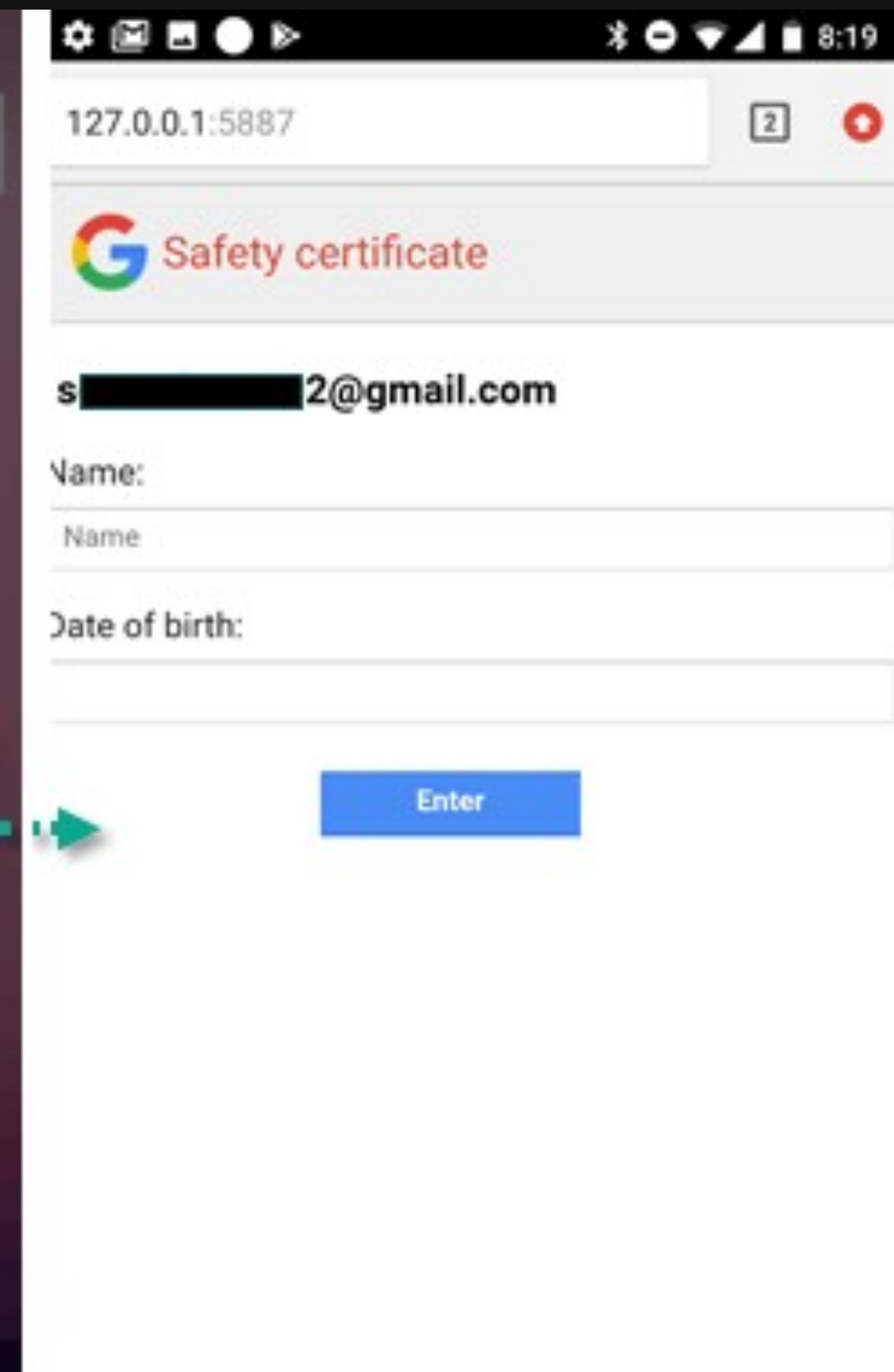
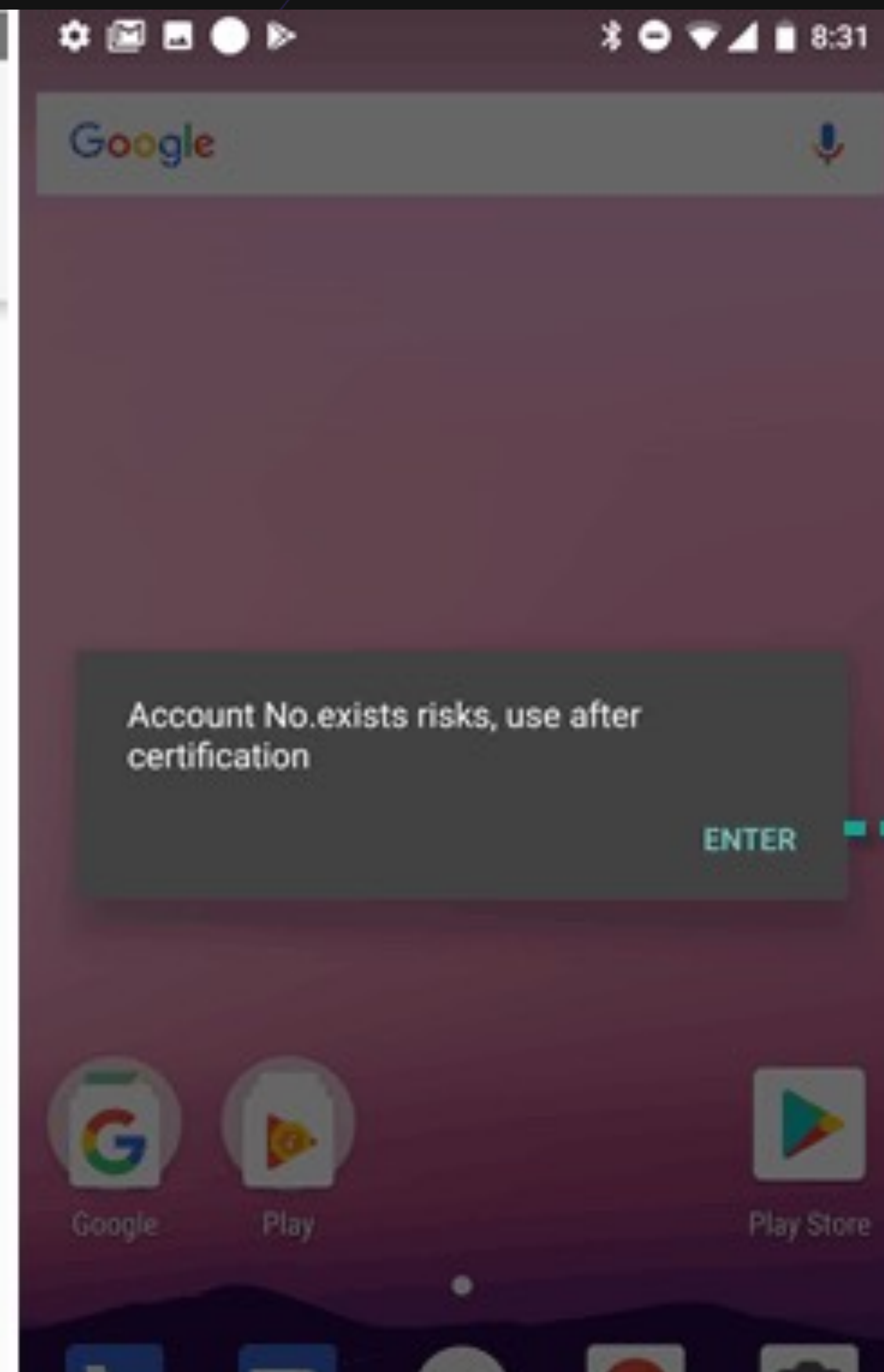
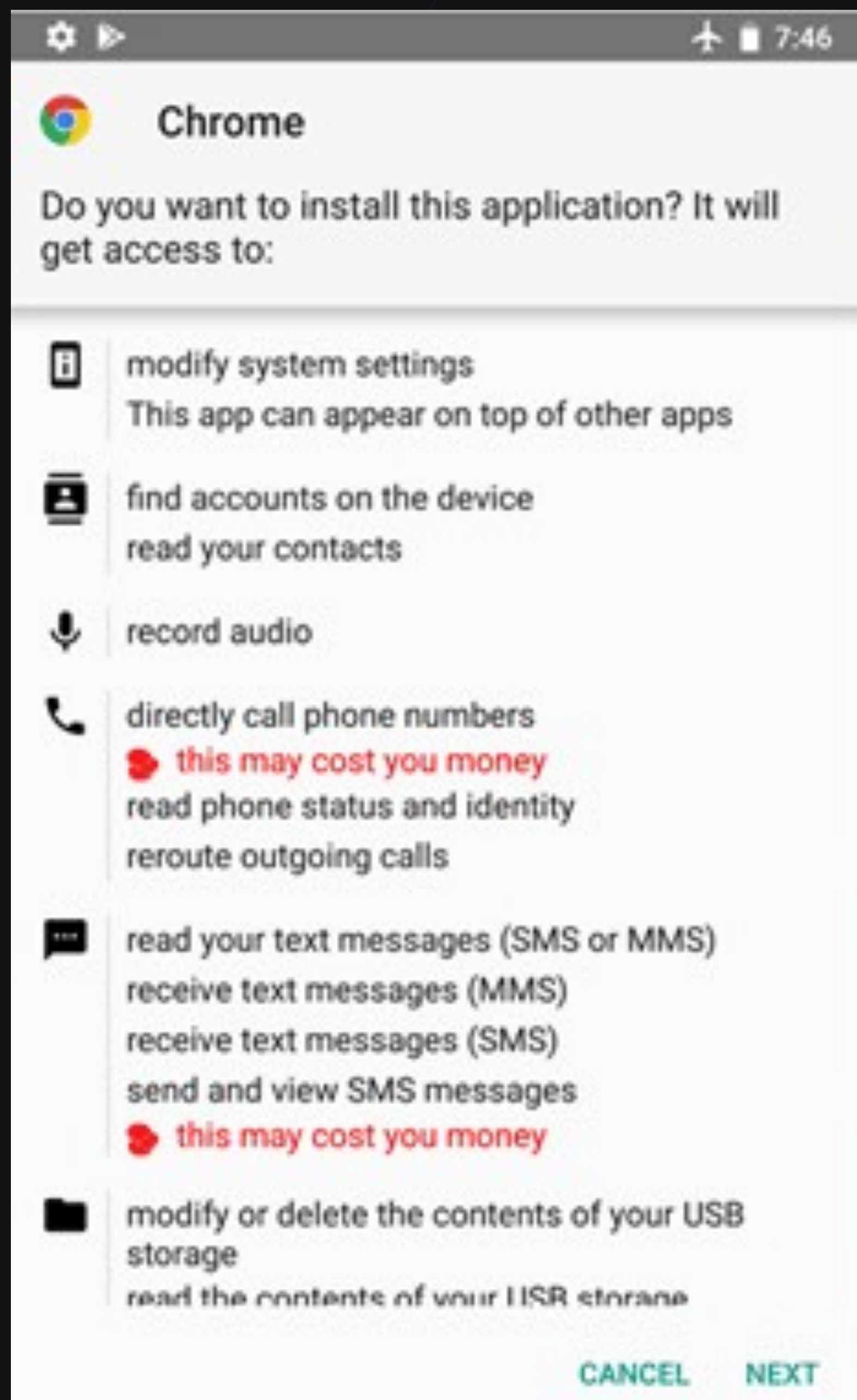
1



securelist.com says:

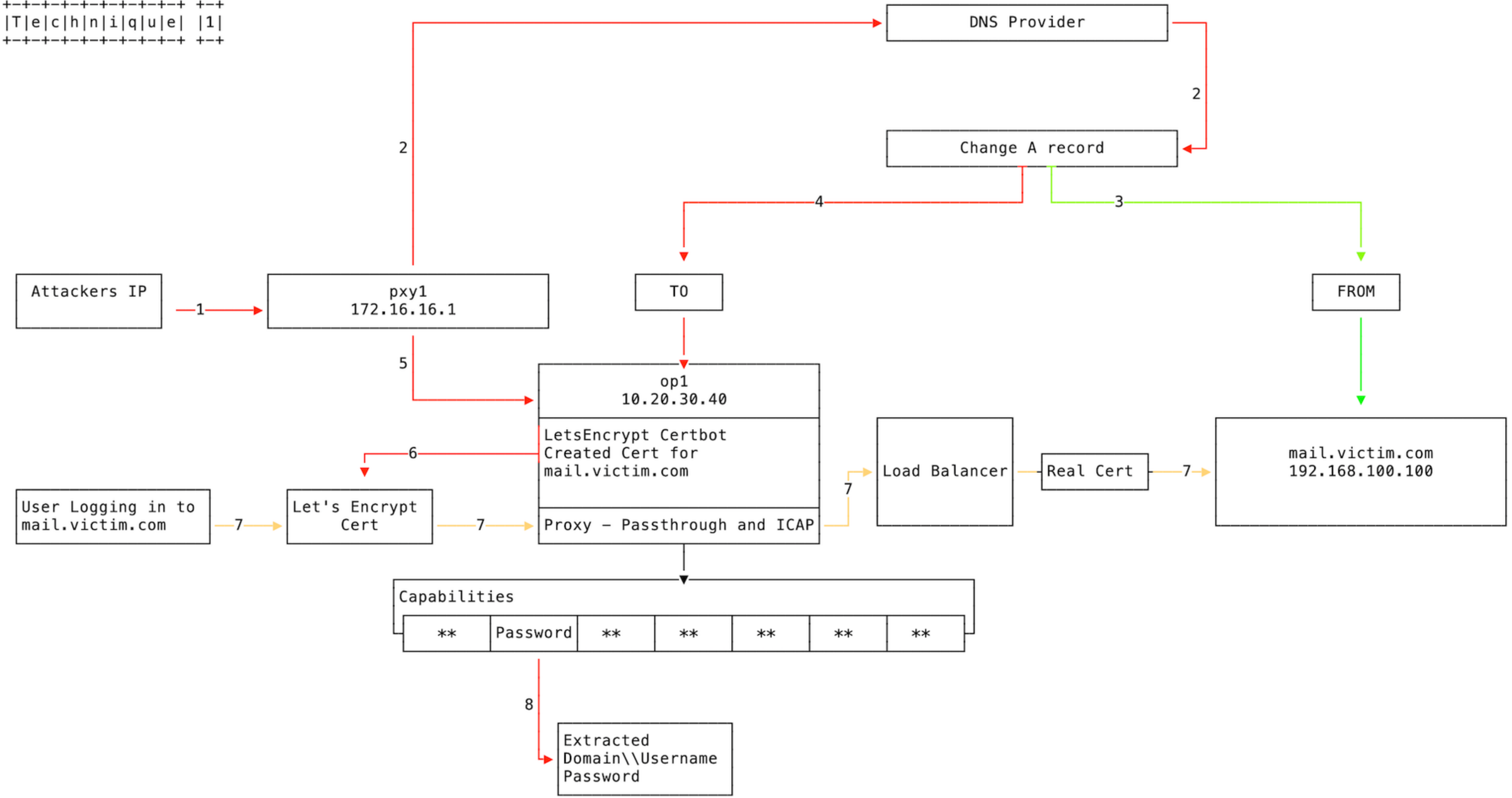
To better experience the browsing, update
to the latest chrome version.

OK



MD5	f3ca571b2d1f0ecff371fb82119d1afe	4d9a7e425f8c8b02d598ef0a0a776a58
Date	March 29 2018	April 7 2018
Legitimate web	http://my.tv.sohu[.]com/user/%s	https://www.baidu[.]com/p/%s/detail
account_IDs	• 329505231 • 329505325 • 329505338	• haoxingfu88 • haoxingfu12389 • wokaixin158998
pattern	"<p>([\u4e00-\u9fa5]+?)</p>\s+</div>"	"公司([\u4e00-\u9fa5]+?)<"
Encrypted dex	\assets\db	\assets\data.sql
Encoding	Base64	Base64 + zlib compression

+-+-+-----+-----+ +-+
|T|e|c|h|n|i|q|u|e| |1|
+-+-+-----+-----+ +-+



ŻÓŁW!!





Kiedy żółw przejmuje DNSy ?

GROUPS

- Overview
- admin@338
- Agrius
- Ajax Security Team
- Akira
- ALLANITE
- Andariel
- Aoqin Dragon
- APT-C-23
- APT-C-36
- APT1
- APT12
- APT16
- APT17
- APT18
- APT19
- APT28
- APT29
- APT3
- APT30
- APT32

[Home](#) > [Groups](#) > Sea Turtle

Sea Turtle

Sea Turtle is a Türkiye-linked threat actor active since at least 2017 performing espionage and service provider compromise operations against victims in Asia, Europe, and North America. **Sea Turtle** is notable for targeting registrars managing ccTLDs and complex DNS-based intrusions where the threat actor compromised DNS providers to hijack DNS resolution for ultimate victims, enabling **Sea Turtle** to spoof log in portals and other applications for credential collection.^{[1][2][3][4]}

ID: G1041

 **Associated Groups:** Teal Kurma, Marbled Dust, Cosmic Wolf, SILICON

Contributors: Inna Danilevich, U.S. Bank; Joe Gumke, U.S. Bank

Version: 1.0

Created: 20 November 2024

Last Modified: 28 March 2025

[Version Permalink](#)

Associated Group Descriptions

Name	Description
Teal Kurma	^{[3][4]}
Marbled Dust	^{[3][4]}
Cosmic Wolf	^{[3][4]}
SILICON	^{[5][4]}

Techniques Used

TECHNIQUES

- Hijack Execution Flow ▾
- Implant Internal Image
- Modify Authentication Process** ^
- Domain Controller Authentication
- Password Filter DLL
- Pluggable Authentication Modules
- Network Device Authentication
- Reversible Encryption
- Multi-Factor Authentication
- Hybrid Identity
- Network Provider DLL
- Conditional Access Policies
- Modify Registry
- Office Application Startup ▾
- Power Settings
- Pre-OS Boot ▾
- Scheduled Task/Job ▾
- Server Software Component ▾
- Software Extensions ▾
- Traffic Signaling ▾
- Valid Accounts ▾
- Privilege Escalation ▾

Procedure Examples

ID	Name	Description
C0046	ArcaneDoor	ArcaneDoor included modification of the AAA process to bypass authentication mechanisms. ^[1]
S0377	Ebury	Ebury can intercept private keys using a trojanized <code>ssh-add</code> function. ^[2]
G1016	FIN13	FIN13 has replaced legitimate KeePass binaries with trojanized versions to collect passwords from numerous applications. ^[3]
S0487	Kessel	Kessel has trojanized the <code>ssh_login</code> and <code>user-auth_pubkey</code> functions to steal plaintext credentials. ^[4]
S0692	SILENTTRINITY	SILENTTRINITY can create a backdoor in KeePass using a malicious config file and in TortoiseSVN using a registry hook. ^[5]

Mitigations

ID	Mitigation	Description
M1047	Audit	Review authentication logs to ensure that mechanisms such as enforcement of MFA are functioning as intended. Periodically review the hybrid identity solution in use for any discrepancies. For example, review all Pass Through Authentication (PTA) agents in the Azure Management Portal to identify any unwanted or unapproved ones.^[6] If ADFS is in use, review DLLs and executable files in the AD FS and Global Assembly Cache directories to ensure that they are signed by Microsoft. Note that in some cases binaries may be catalog-signed, which may cause the file to appear unsigned when viewing file properties.^[7] Periodically review for new and unknown network provider DLLs within the Registry (<code>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<NetworkProviderName>\NetworkProvider\ProviderPath</code>). Ensure only valid network provider DLLs are registered. The name of these can be found in the Registry key at <code>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order</code>, and have corresponding service subkey pointing to a DLL at <code>HKEY_LOCAL_MACHINE\SYSTEM\CurrentC ontrolSet\Services\<NetworkProviderName>\NetworkProvider</code>.
M1032	Multi-factor Authentication	Integrating multi-factor authentication (MFA) as part of organizational policy can greatly reduce the risk of an adversary gaining control of valid credentials that may be used for additional tactics such as initial access, lateral movement, and collecting information. MFA can also be used to restrict access to cloud resources and APIs.

CO W TYM WOW ?

Cache nietknięty

TLS - „na zielono” - end user nie złapie

Słabość łańcucha dostaw (SPF)

Kredki wykradzione od VPNów, OWA, banki+public
kierują do giełd i koparek

JAKIE REDIRECTY



WARIACIE ??

U MNIE DZIAŁA

CO W TYM WOW ?

Cache nietknięty

TLS - "end user nie złapie"

Struktura dostaw (SPF)

Kredki wykraśnięte z VPNów, OWA, banki+public

o giełd i koparek

Zewnętrzny monitoring

- 1** Badamy końcowy rezultat współdziałania wszystkich systemów odpowiedzialnych za daną funkcjonalność – badamy pełne cyfrowe procesy z punktu widzenia klienta końcowego.
- 2** Monitorujemy z wielu miejsc w Polsce i na świecie, z łącz różnych operatorów, również mobilnych, niezależnie od infrastruktury naszych Klientów. Uzupełniamy wewnętrzne systemy monitorowania, wykrywając awarie, których nie zauważają inne systemy.
- 3** W ramach usługi dostarczamy zarówno system monitorowania jak i support techniczny naszych inżynierów pomagających w analizie przyczyn awarii i rozwiązywaniu kwestii dostępności oraz aktualizacji scenariuszy.

Podsumowanko

1. **Mniej znaczy lepiej. Monitoruj kluczowy proces na ważnym etapie (zamiast odbierać setki alertów).**
2. **Zdefiniuj kryteria sukcesu, dla każdego etapu scenariusza.**
3. **Alertuj właściwą osobę. Definiuj ścieżkę eskalacji.**
4. **Backup! Pomyśl o dwóch niezależnych systemach monitoringu.**
5. **Gdy napotkasz ścianę, próbuj POCa innych rozwiązań. Szukaj McGyverów.**

Formy współpracy - Kanał Partnerski

W Monit24 jesteśmy otwarci współpracy partnerkiej w różnych wariantach aby jak najlepiej dostosować się do twoich klientów i twojego procesu sprzedaży.

1. **Reference** - rozbuduj swoją ofertę.

Dodaj nasze rozwiązanie do swojej oferty – w formie white label lub jako element marketplace.

2. **Reseller** - szybki start i gotowe wsparcie

To najpopularniejszy model na start. Zapewniamy Ci pełne wsparcie sprzedażowe i obsługowe – od pierwszej rozmowy po finalizację sprzedaży. To najprostszy model współpracy.

3. **Integrator (MSP)** - rozwijaj swój biznes w oparciu o Monit24

Monit24 nie tylko technologia – to gotowe narzędzie do tworzenia nowych źródeł przychodu w oparciu o monitoring i konsulting. Otrzymasz szkolenia zespołu sprzedażowego i technicznego, dostęp do naszej wiedzy i wsparcie w budowaniu Twojej własnej linii biznesowej.

Proces dla nowego partnera

Umowa partnerska

Onboarding (szkolenie produktowe, nadanie dostępów do portalu partnerskiego)

Rejestracja projektu i kwalifikacja

POC lub jego przedłużenie i podsumowanie

Wycena

Zamówienie lub umowa z klientem

Podstawowe zasady kanału partnerskiego

Rejestracja projektu - minimum 90 dni od zaakceptowania

Partner preferowany - odpowiedzialny za pierwszą sprzedaż i opiekę nad utrzymaniem klienta

Partner niepreferowany - każdy partner zgłaszający się po wycenę i spełniający kryteria wyceny dla klienta

Punkty przewagi - umówienie spotkania, przekazanie oferty, nadzorowanie procesu sprzedaży

Szkolenia

Bezpłatne szkolenia zespołów sprzedażowych i technicznych – pomagamy Twoim handlowcom zdobyć wiedzę i umiejętności, które realnie przekładają się na wyniki sprzedaży.

Szkolenia certyfikowane - potwierdzają wiedzę i umiejętności twojego zespołu.

Dedykowany partner account manager - to twój łącznik z Monit24

Akademia Monit24 - to cykliczne spotkania dla wybranych partnerów gdzie dzielimy się wiedzą i świetnie spędzamy czas.

Dostęp do unikatowego know-how – dzielimy się wiedzą, którą zdobywamy od 14 lat współpracy z naszymi klientami abyś unikał błędów i szybciej osiągał sukcesy.

Case studies – udostępniamy sprawdzone strategie i przykłady sukcesów, które możecie wykorzystać w swoich działaniach.

Pomoc na każdym kroku procesu sprzedaży – od pierwszego kontaktu z klientem po finalizację umowy, zapewniamy pełne wsparcie i doradztwo.

Portal partnerski – dajemy dostęp do nowoczesnego narzędzia aby efektywnie zarządzać projektami, usprawnić współpracę i zminimalizować kwestie sporne w kanale.

Not For Resale

W Monit24 oferujemy produkty w opcji Not For Resale. Umożliwi to korzystanie i sprawdzenie funkcjonalności Monit24 na własnych aplikacjach, ułatwi demonstrację klientom a przede wszystkim, będzie stanowić własne laboratorium testowe. Produkty zakupione w formie Not For Resale podlegają specjalnym rabatom lub są w pełni bezpłatne na użytek własny.

NIE STRACISZ BACKUPÓW

JEŚLI NIE ROBISZ BACKUPÓW

Zapytaj mnie o monitoring.



Mateusz Ossowski

Channel Sales Director

509 746 430

mateusz.ossowski@monit24.pl



<https://cloud.google.com/blog/topics/threat-intelligence/global-dns-hijacking-campaign-dns-record-manipulation-at-scale/>
<https://thehackernews.com/2025/06/zero-click-ai-vulnerability-exposes.html>
<https://attack.mitre.org/techniques/T1556/>
https://www.wired.com/2008/11/ff-kaminsky/?utm_source=chatgpt.com
<https://attack.mitre.org/groups/G1041/>