NASK

Wyzwania w zakresie monitoringu bezpieczeństwa aplikacji bankowości mobilnych

NASK-PIB

Warszawa | maj 2023 r.

nask.pl

Obszary działalności NASK

Projekty
Strategiczne

Security
IT/OT

Badania
i Rozwój

Edukacja
i działalność
non-profit

Telekomunikacja

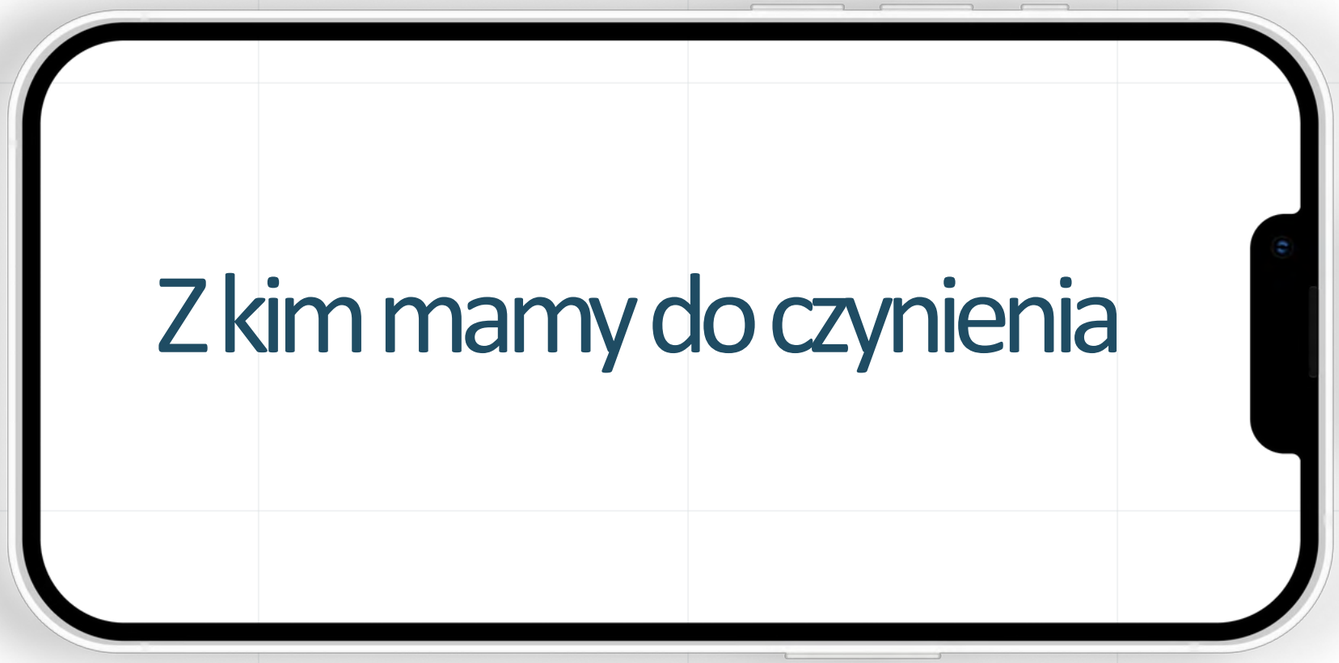
Obsługa domeny
krajowej .pl

NASK

AGENDA

1. Z kim mamy do czynienia
2. Statystyki
3. Funkcjonalności rodzin złośliwego oprogramowania
4. Sposoby infekcji
5. Ataki typu Overlay” i „zdalny pulpit”
6. Narzędzie do ochrony urządzeń mobilnych
7. Usługa CTI - Collective Threat Intelligence

NASK



NASK

MOST WANTED

Ten Most Wanted Fugitives | Fugitives | Capitol Violence | Terrorism | Kidnappings/Missing Persons | Parental Kidnappings | More

Crimes Against Children | Murder | Additional Violent Crimes | Cyber | White Collar Crimes | Counterintelligence | CEI | Human Trafficking

Cyber's Most Wanted

Select the images of suspects to display more information.

Filter by

Filter by: Filter by title, description, category...

Year

Filter

Sort by: Newest

Results: 119 Items

MINH QUỐC NGUYỄN

UGO CAESAR ANELE

IRANIAN CYBER ACTORS

MANSOUR AHMADI

AHMAD KHATIBI AGHDA

AMIR HOSSEIN NICKAEIN RAVARI

EMILIO JOSE CORREDOR LOPEZ

MOISES LUIS ZAGALA GONZALEZ

EVGENY VIKTOROVICH GLADKIKH

RUSSIAN FSB CENTER 16 HACKERS

PAVEL ALEKSANDROVICH AKULOV

MIKHAIL MIKHAILOVICH GAVRILOV

MARAT VALERYEVICH TYUKOV

IGOR DEKHTYARCHUK

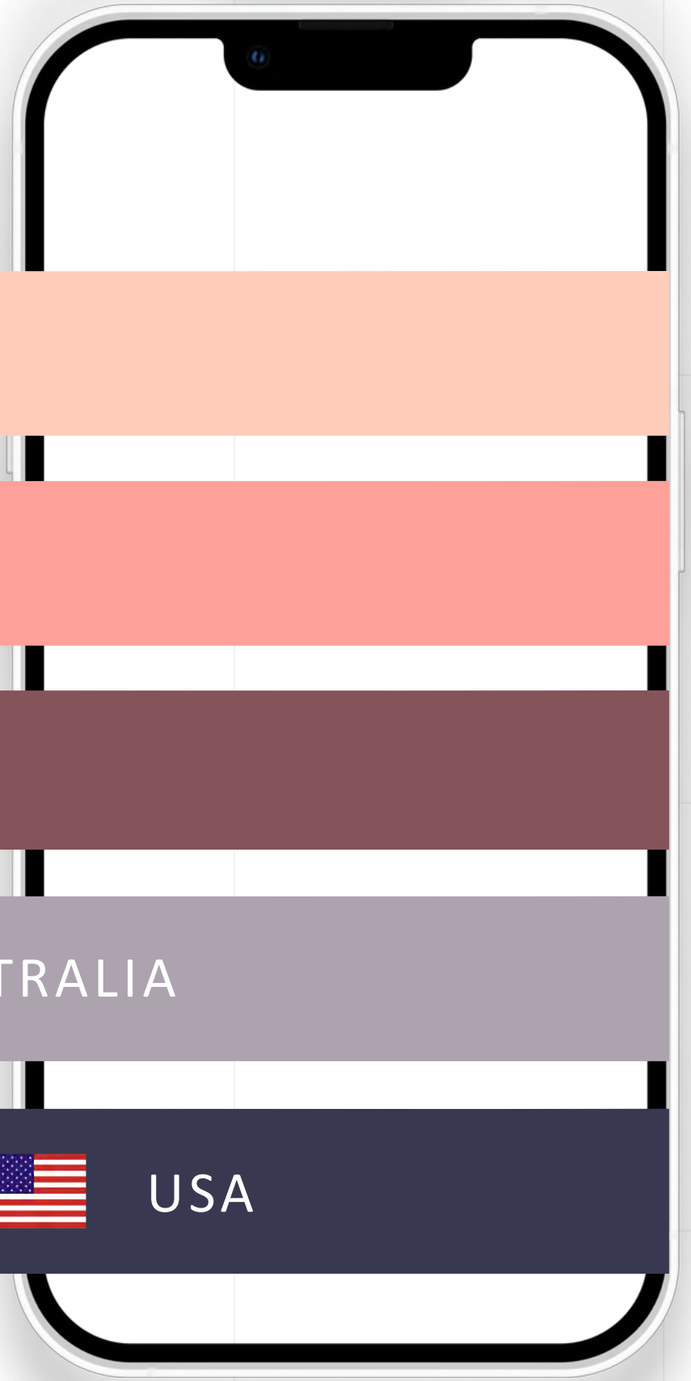
IRANIAN INTERFERENCE IN 2020 U.S. ELECTIONS

NASK

SOURCE
www.fbi.gov

NASK

NAJCZĘSTSZE CELE ATAKÓW



- HISZPANIA
- TURCJA
- POLSKA
- AUSTRALIA
- USA

NASK

SOURCE
www.threatfabric.com

2017 LOKIBOT

CERBERUS

FLUBOT

BLACKROCK

S.O.V.A

HYDRA

2023 HOOKBOT, XENOMORPH

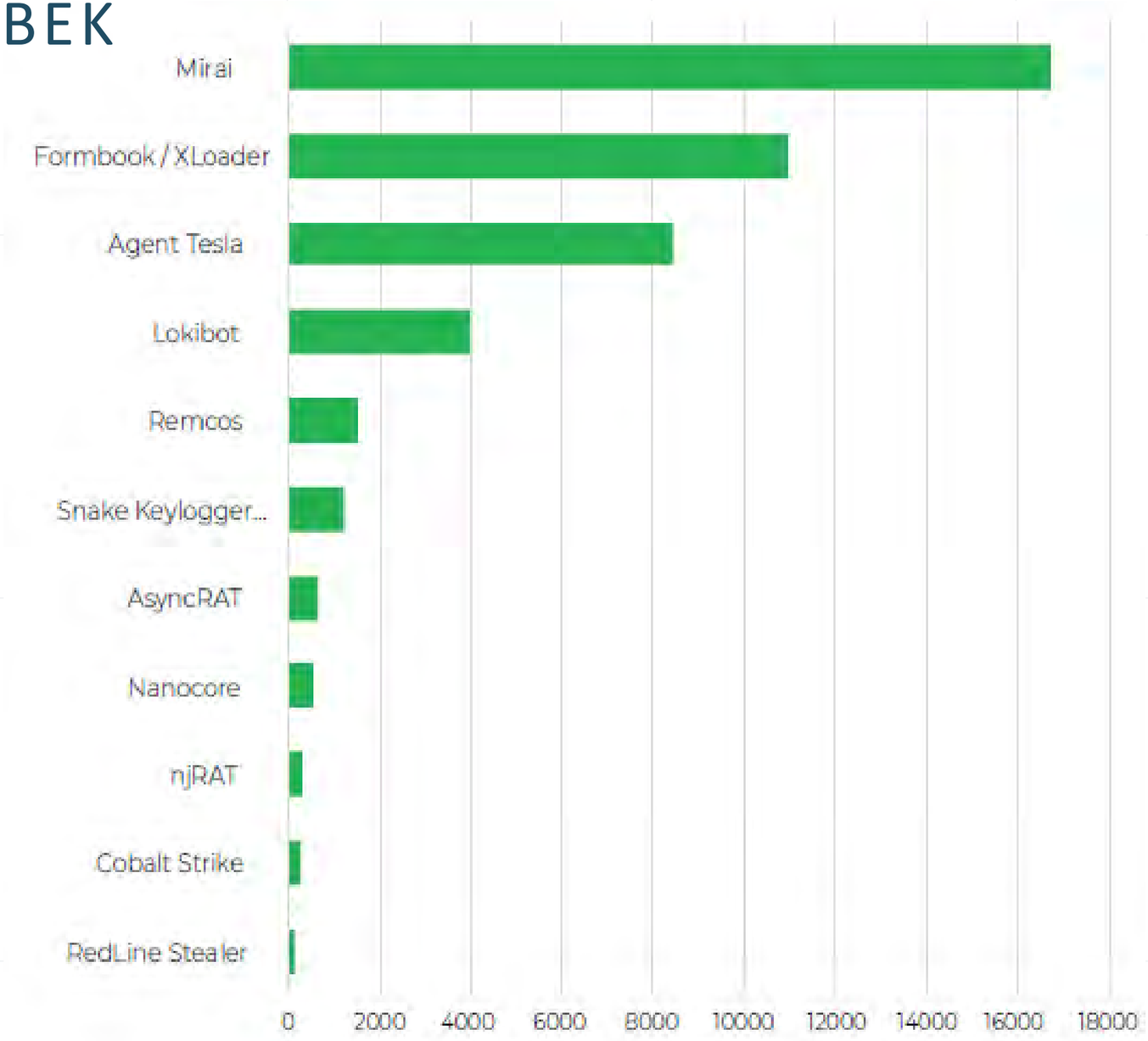
w 2022 roku

196 000

próbek

SOURCE
www.kaspersky.com

10 RODZIN ZŁOŚLIWEGO OPROGRAMOWANIA Z NAJWIĘKSZĄ LICZBĄ PRÓBEK



SOURCE
www.cert.pl

NASK

NASK

GŁÓWNE FUNKCJONLANOŚCI RODZIN MOBILE MALWARE

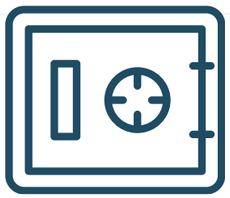
OVERLAY

KEYLOGGER

SMS

CONTACTS

CALL CONTROL



2FA STEALING

GEOLOCATION

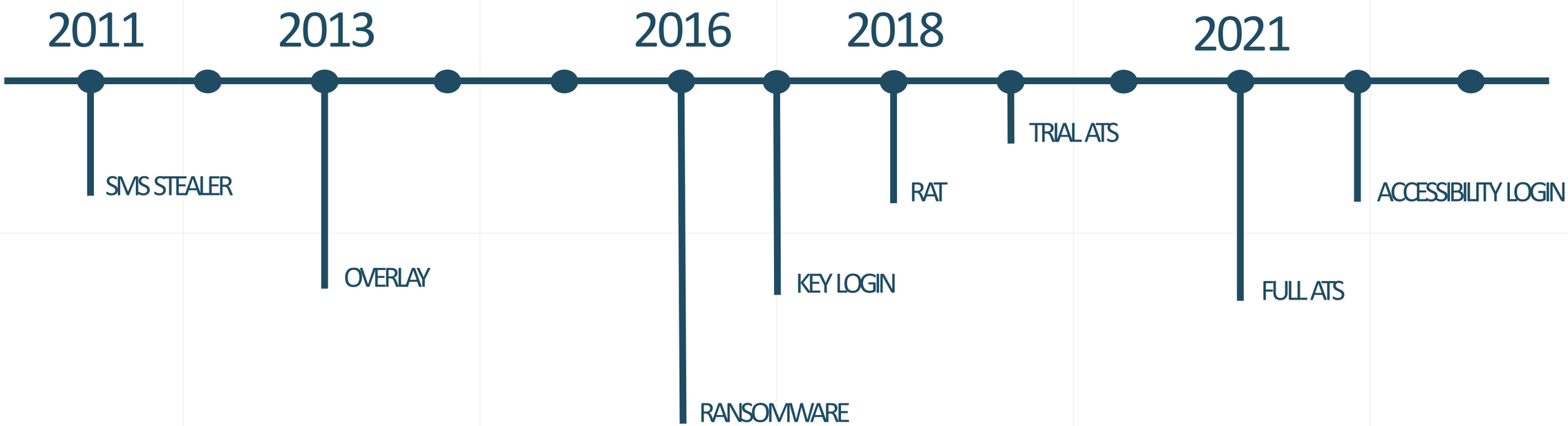
COOKIES STEALER

RAT

FUTURE FEATURES

NASK

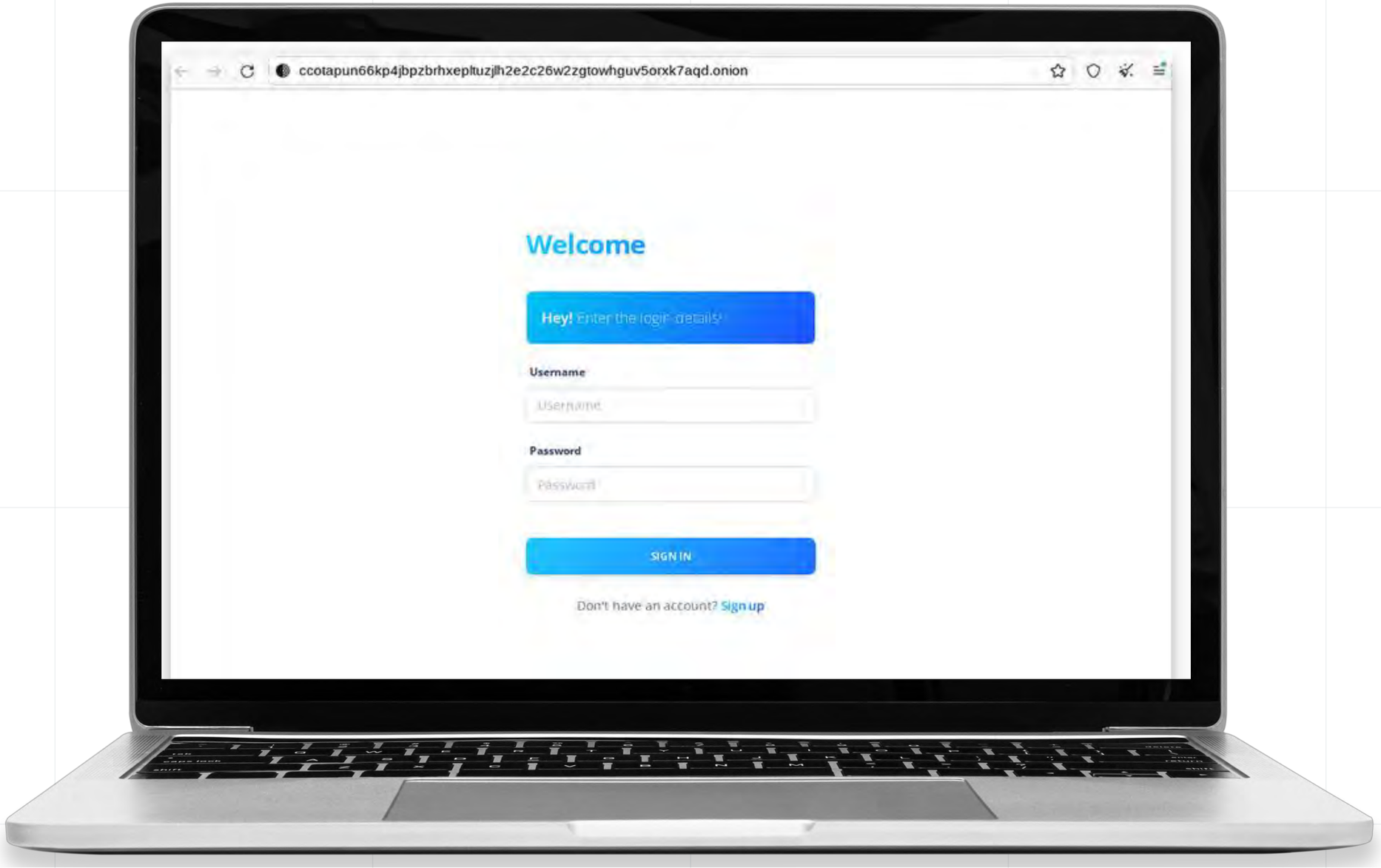
EWOLUCJA FUNKCJONLANOŚCI ANDROID MALWARE



2023

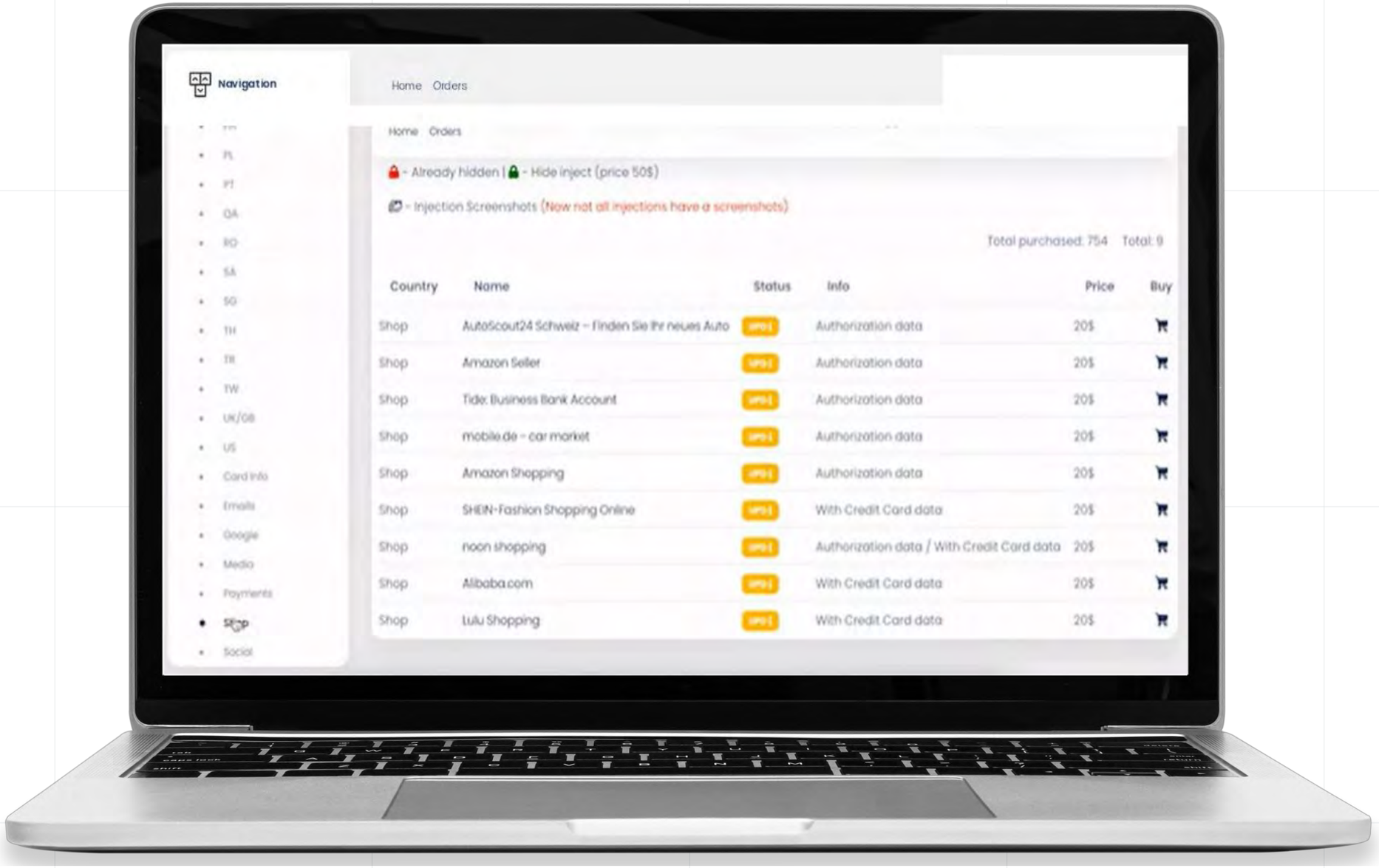
SOURCE
www.threatfabric.com

MALWARE AS A SERVICE (MaaS) – IN THE BOX



NASK

MALWARE AS A SERVICE (MaaS) – IN THE BOX



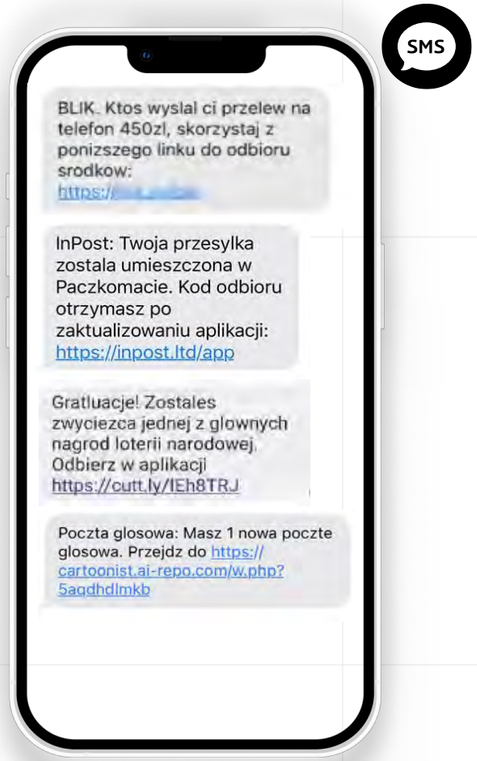
NASK

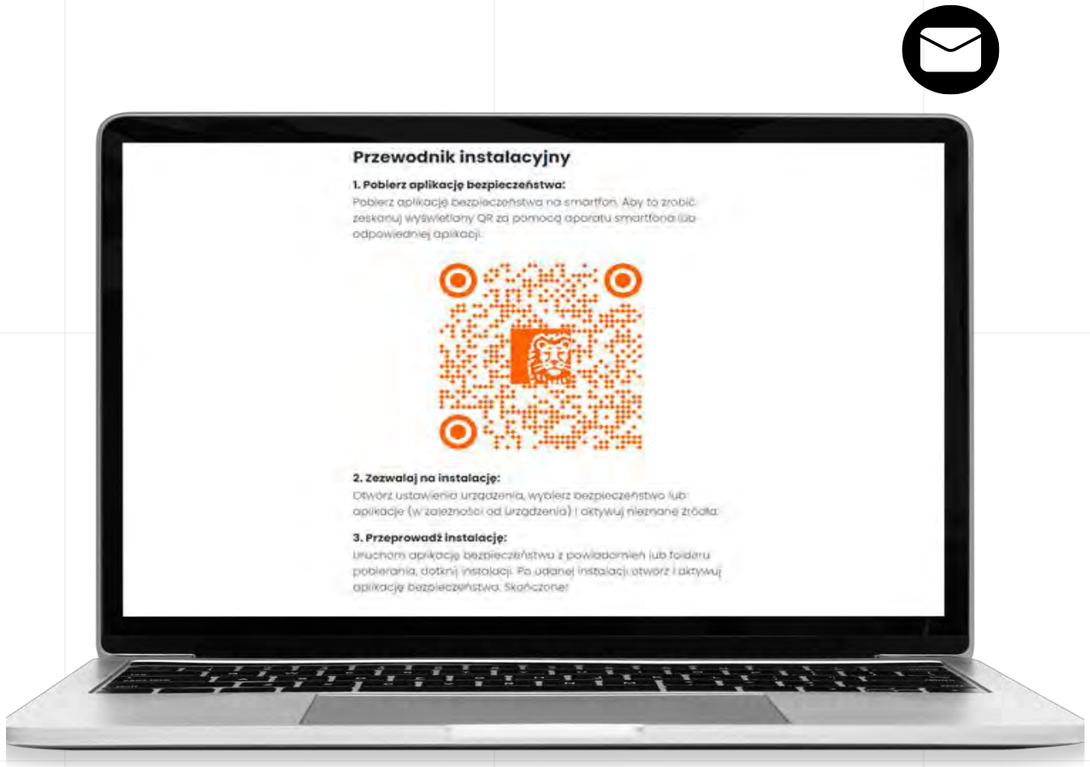
ATS – AUTOMATIC TRANSFER SYSTEM

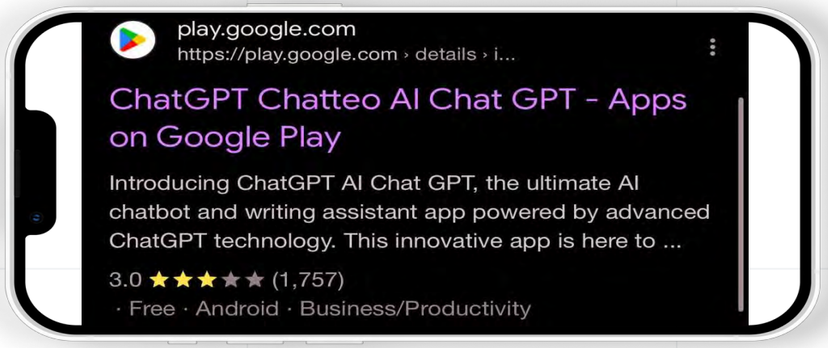
NASK

NASK

SPOSOBY INFEKCJI

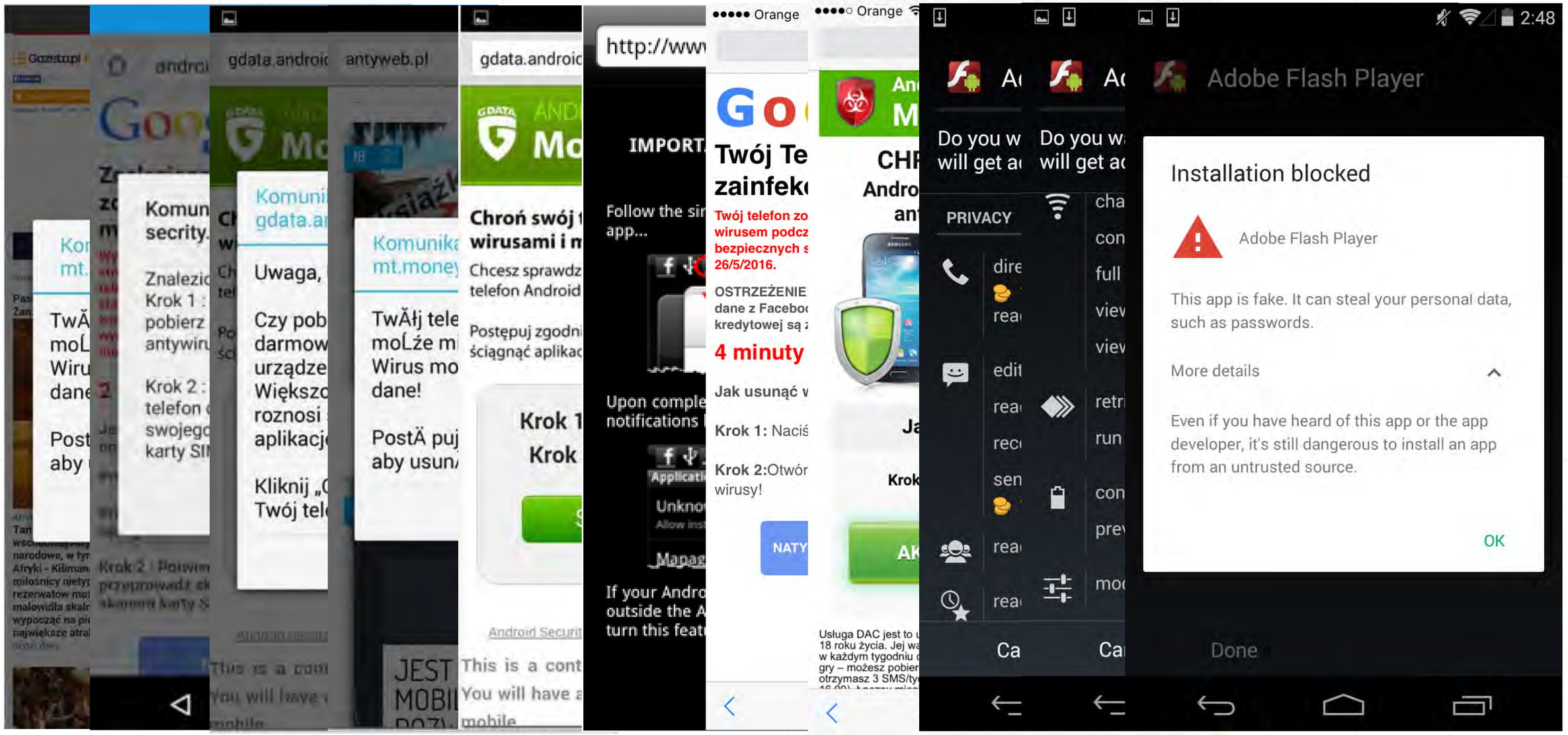




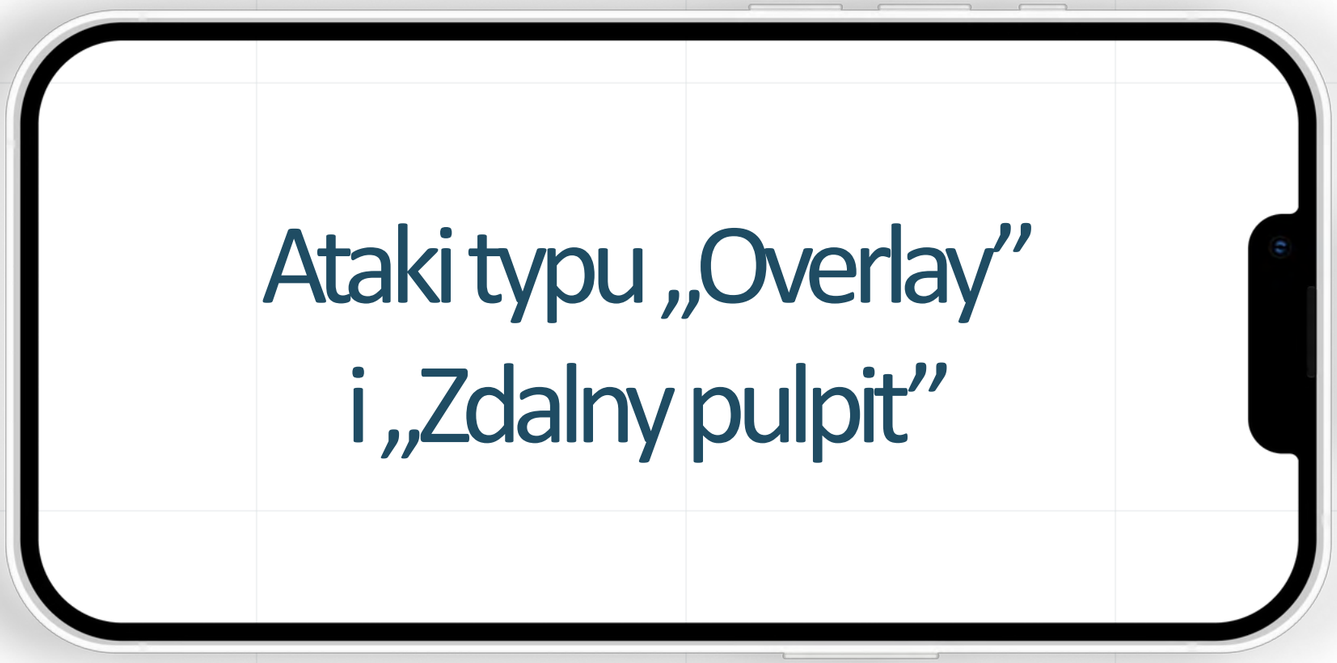


NASK

SPOSOBY INFEKCJI

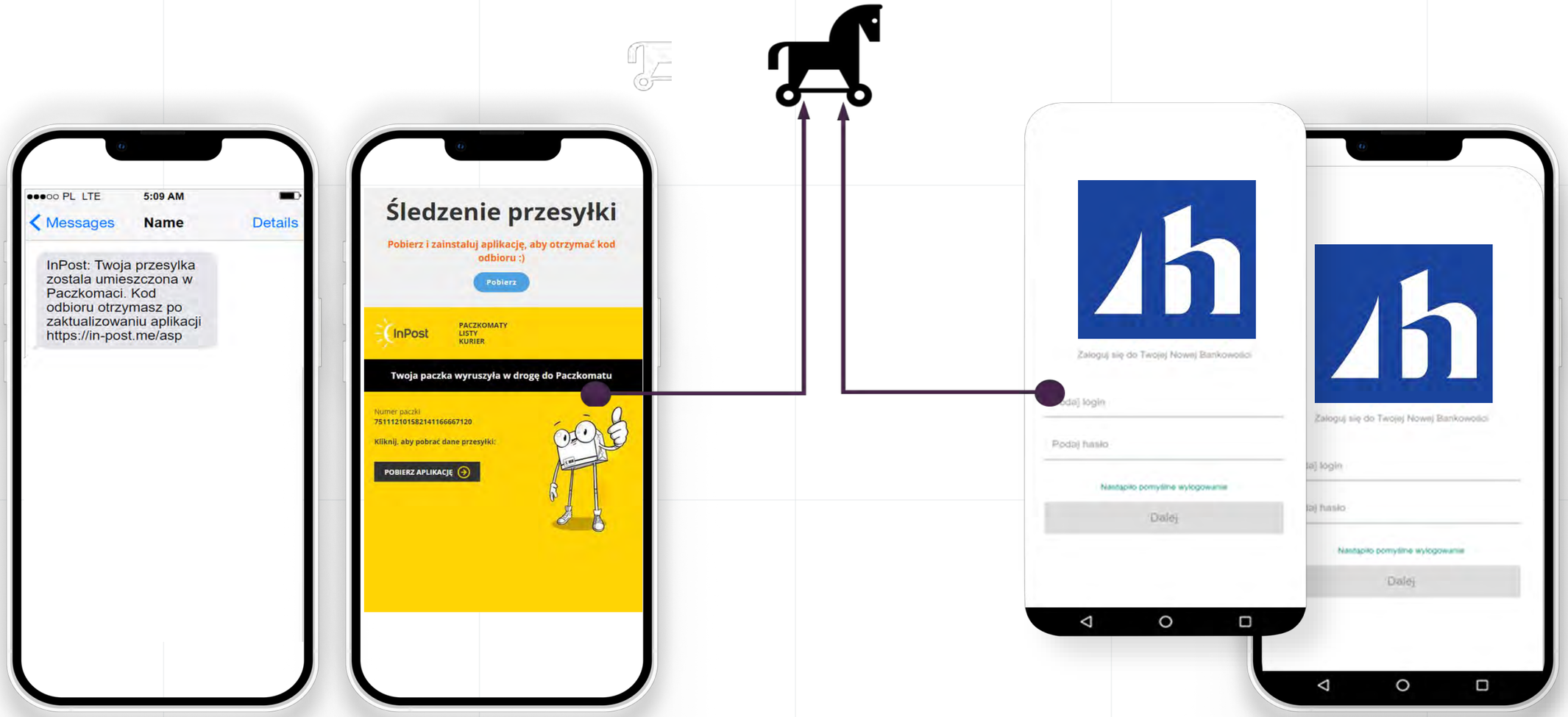


NASK



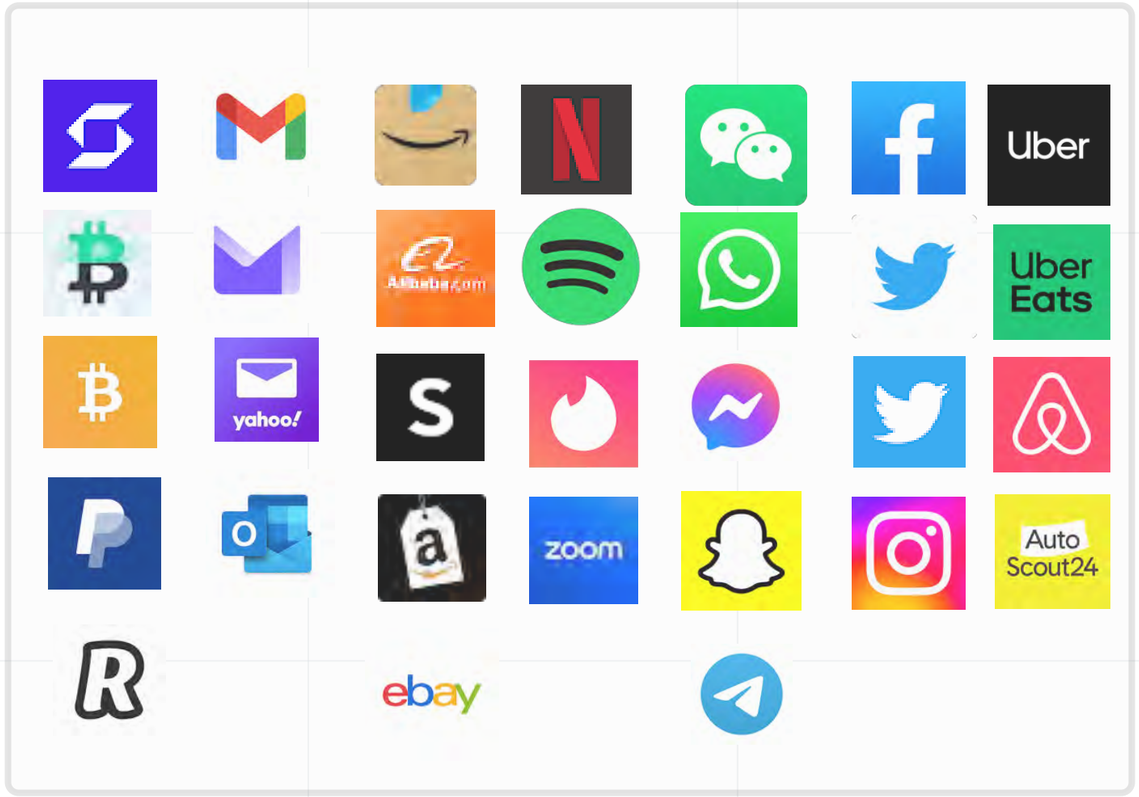
NASK

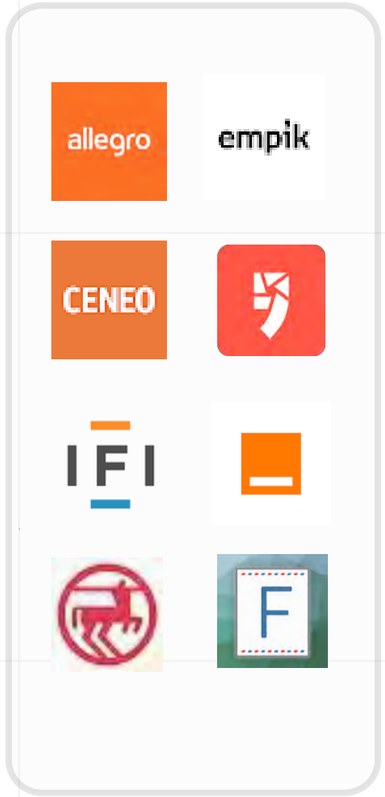
OVERLAY

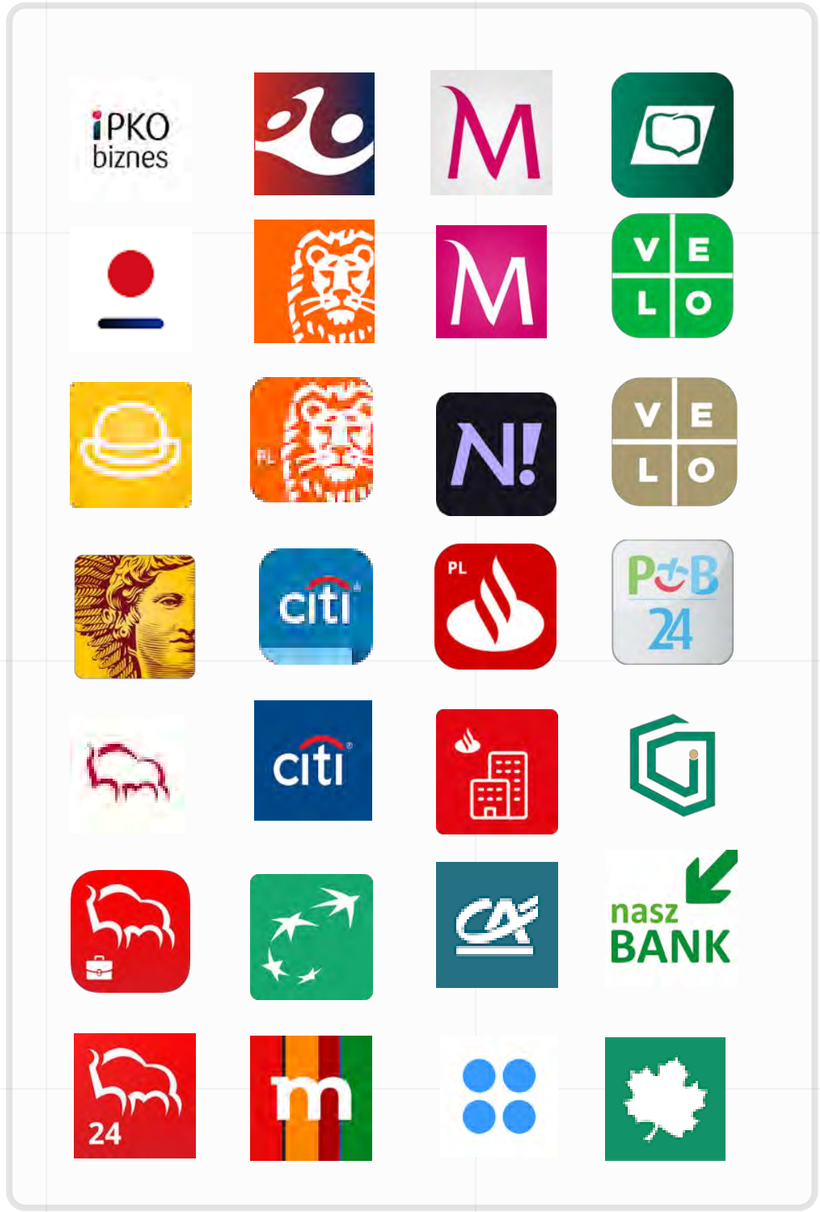


NASK

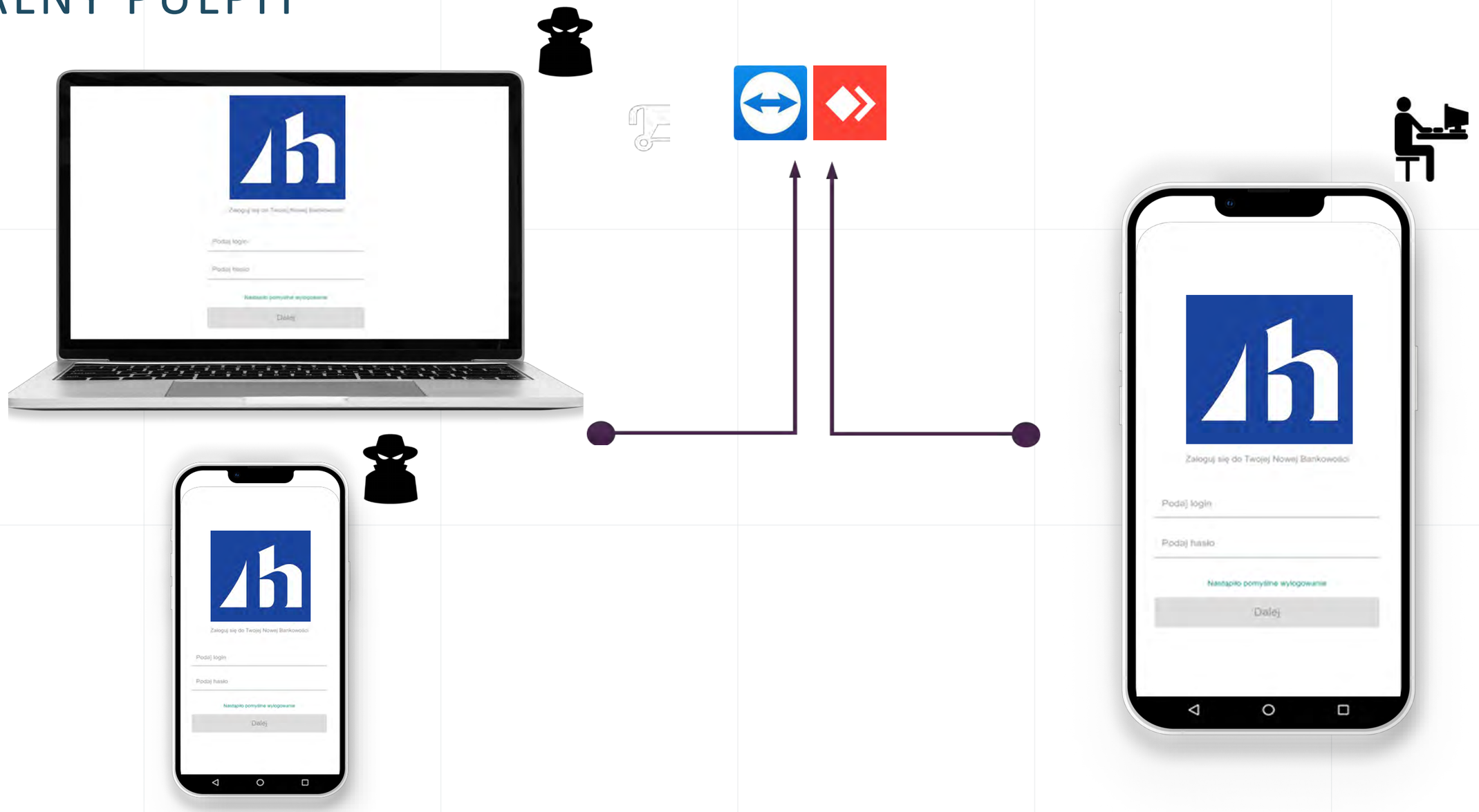
WYBRANE NAKŁADKI (OVERLAY) NA APLIKACJE







ZDALNY PULPIT



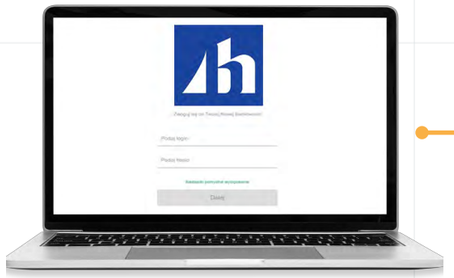
NASK

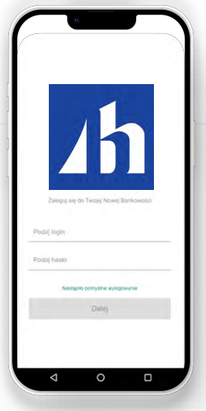
NASK

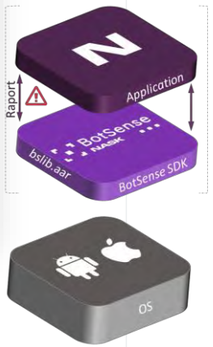
SYSTEM BOTSENSE

BotSense
NASK

CTI Mobile Malware
Feed as Service







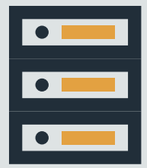
Skrypt BotSense

Raport z ID i wersjami przeglądarki, SO, itp.

Konfiguracja
BotSense

BotSense
Management
System

BotSense GUI



Infrastruktura Klienta:
baza danych, SIEM,
Antyfraud

Administrator

Infrastruktura
Banku

NASK

FUNKCJONALNOŚCI SYSTEMU BOTSENSE

Wykrywa trojany bankowe w atakach MiTB

Wykrywa podmiany nr konta (Bnatrix, VBKlip)

Wykrywa podstawowe ataki phishingowej (kopia strony)

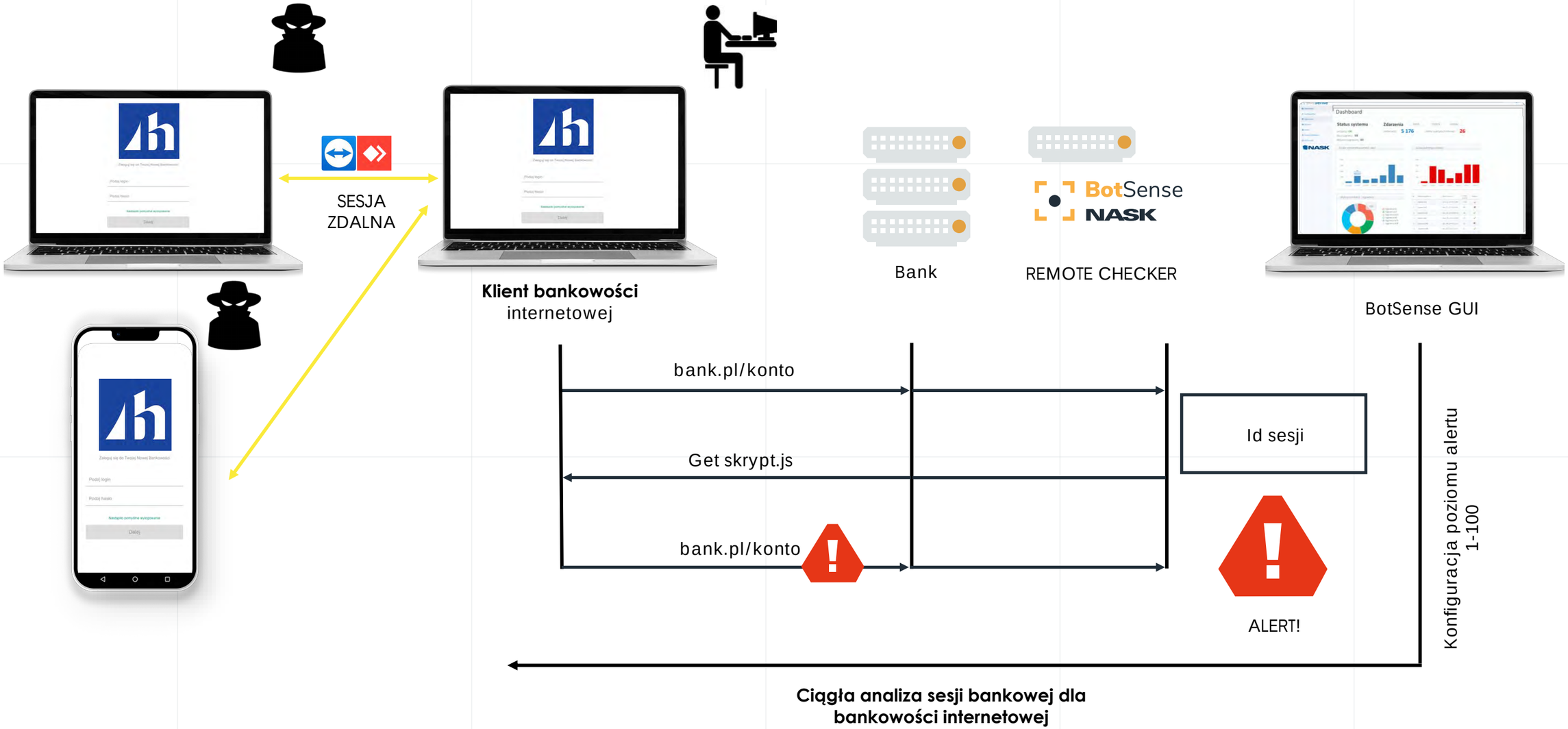
Wykrywa ataki **„zdalny pulpit”**

Dostarcza fingerprint **urządzenia i przeglądarki**

Raporty

BotSense
NASK

WYKRYWANIE ZDALNEGO PULPITU PRZEZ SYSTEM BOTSENSE



BotSense
NASK

FUNKCJONALNOŚCI SYSTEMU BOTSENSE MOBILE

Wykrywanie mobile malware

- Wykrywanie złośliwych aplikacji za pomocą Blacklisty
- Wykrywanie aplikacji z uprawnieniami do czytania SMS
- Wykrywanie aplikacji z określonymi uprawnieniami

Weryfikacja integralności urządzenia

- Wykrywanie uprawnień root na telefonie
- Wykrywanie emulatora systemu operacyjnego (brak fizycznego urządzenia)
- Fingerprint urządzenia

Weryfikacja integralności chronionej aplikacji

- Wykrywanie przesłaniania chronionej aplikacji (Overlay)
- Obsługa procesu blokowania przekazywania ekranu aplikacji przy dostępie zdalnym
- Wykrywanie trybu debugowania chronionej aplikacji
- Sprawdzanie kanału instalacji

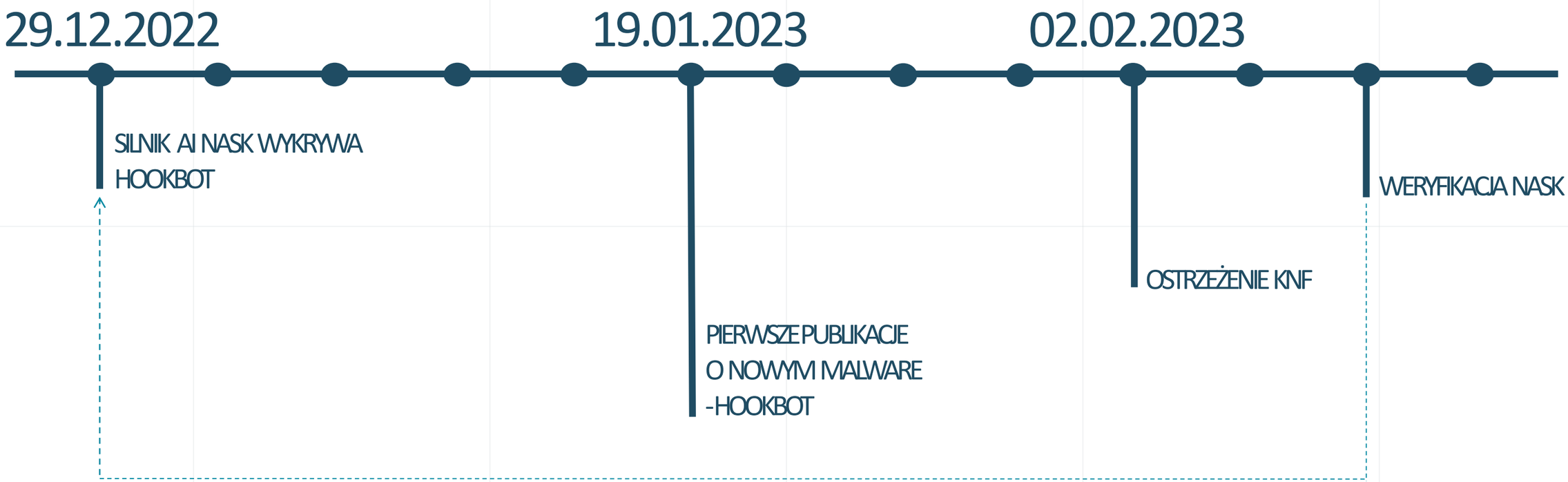
Weryfikacja ustawień sieciowych

- Informacja o położeniu geograficznym urządzenia
- Badanie poziomu bezpieczeństwa sieci WiFi
- Rejestracja kanałów dostępu do Internetu (w tym roaming)

Raporty

BotSense Mobile
NASK

CASE STUDY – NOWY MODUŁ AI WYKRYWA MALWARE HOOKBOT



BotSense Mobile
NASK

PLANY ROZWOJOWE BOTSENSE

- Nowy Moduł Malware Hunter^{AI} wykrywania złośliwych aplikacji mobilnych za pomocą metod AI
- Nowy Moduł **Pasword** Checker bazująca na biometrii behawioralnej weryfikujący użytkownika bankowości www **podczas jego logowania do konta**
- Nowy Moduł wykrywania zdalnych sesji za pomocą AI wspartych o budowanie profili użytkowników bankowości www
- Nowy Moduł biometrii twarzy, dłoni, tęczówki oka oraz głosu
- Nowy Moduł Biometrii Behawioralnej dla bankowości **Internetowej oraz mobilnej**
- Stworzenie profilu przestępcy na bazie Biometrii Behawioralnej i dzielenie się nim wśród pozostałych użytkowników BotSense

BotSense
NASK

NASK

Usługa CTI - Collective Threat Intelligence

INCIDENT RESPONSE

BRAND PROTECTION

FRAUD PREVENTION
(FOR BANKS ONLY)

VULNERABILITY SCAN

FEED AS SERVICE

REPORT

ADVANCED THREAT
ANALYSIS

NASK

Dziękuję

Piotr Kot
zastępca Dyrektora Działu
Rozwoju Biznesu

+48 608 564 711
piotr.kot@nask.pl

nask.pl