Phishing jako usługa – demaskowanie ekosystemu kampanii phishnigowych

Wstęp

W trakcie prowadzonych działań, zespół CSIRT KNF zidentyfikował oraz przeprowadził szczegółową analizę kampanii phishingowej. Natrafiliśmy na sieć wzajemnie powiązanych fałszywych stron, które wyróżniają się globalnym zasięgiem i są dystrybuowane w różnych krajach na całym świecie. Cyberprzestępcy w ramach tej kampanii wykorzystywali wizerunek znanych i zaufanych instytucji pocztowych, serwisów streamingowych oraz operatorów telekomunikacyjnych co znacząco podnosiło skuteczność ich działań.

W Polsce, podobnie jak w innych krajach, obserwowaliśmy fałszywe wiadomości, nakłaniające ofiary do kliknięcia w złośliwe linki, prowadzące do stron wyłudzających dane finansowe oraz osobowe.

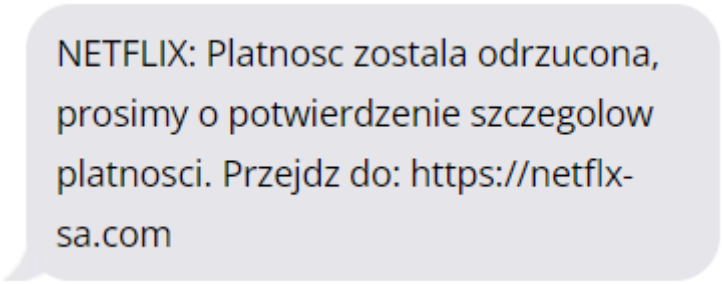
Przeprowadzona przez nas analiza umożliwiła nie tylko zidentyfikowanie kluczowych elementów infrastruktury wykorzystywanej przez cyberprzestępców, ale także odkrycie narzędzi zarządzania kampanią, w tym paneli administracyjnych. Ujawniliśmy również mechanizmy pozwalające atakującym na blokowanie dostępu z niepożądanych lokalizacji, co jest świadectwem ich technik unikania detekcji.

Analiza ma na celu podkreślenie znaczenia ciągłego monitorowania przestrzeni cybernetycznej i adaptacji metod obronnych do szybko zmieniającego się środowiska zagrożeń. Współpraca międzynarodowa i wymiana wiedzy między organizacjami zajmującymi się cyberbezpieczeństwem jest kluczowa w efektywnym przeciwdziałaniu tego typu złożonym atakom phishingowym, które stanowią coraz większe wyzwanie dla bezpieczeństwa danych użytkowników na całym świecie.

KAROL PACIOREK
PATRYK BARYSZEWSKI
MATEUSZ GRUSZKIEWICZ

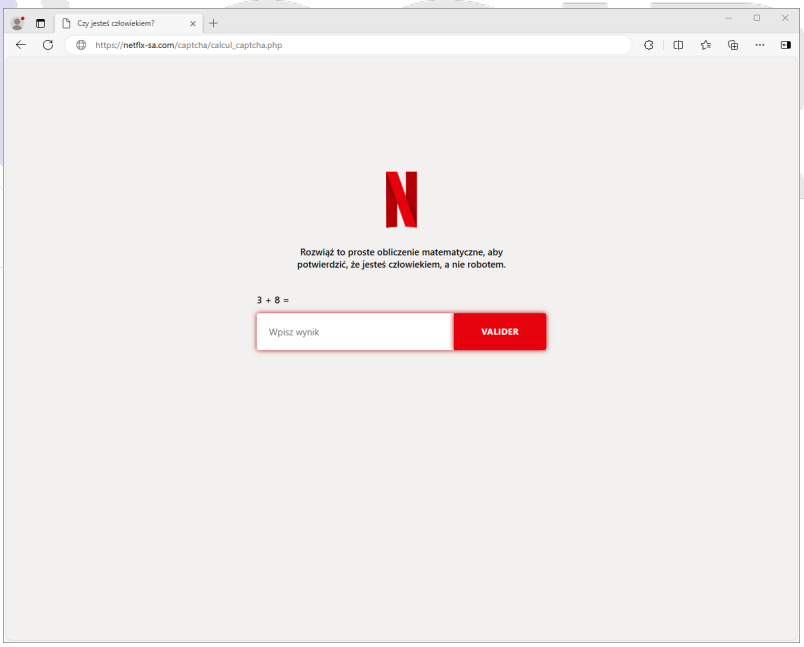
Scenariusz Ataku

W omawianym przykładzie domeny dystrybuowane są przy pomocy wiadomości SMS, jednak nie wykluczamy użycia innych form dystrybucji np. mail lub komunikatory internetowe.



1. Fałszywa wiadomość SMS.

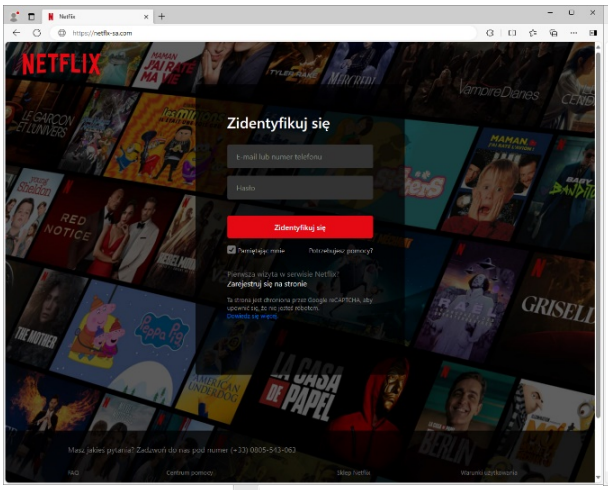
Po przekierowaniu na stronę phishingową, użytkownicy często spotykają się z mechanizmem CAPTCHA – testem, który ma na celu odróżnienie ludzi od automatów.



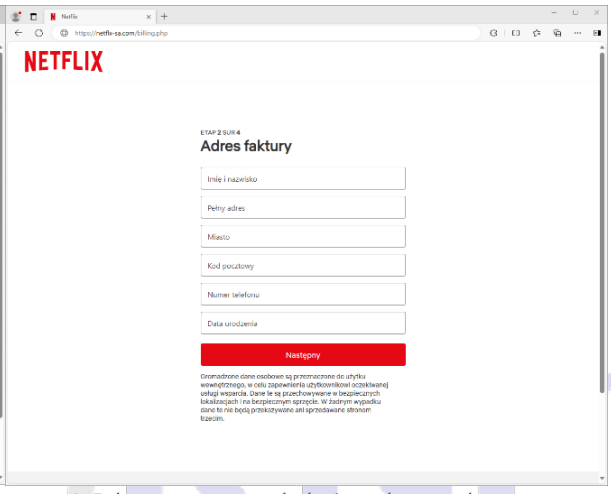
2. Fałszywa strona z CAPTCHa.

W kontekście phishingu, CAPTCHA służy jako metoda zabezpieczająca przed automatycznymi narzędziami wyszukiwania i analizy stron internetowych, które mogłyby wykryć i zgłosić złośliwą zawartość.

Po pokonaniu CAPTCHA, użytkownicy są przekierowywani na stronę phishingową, która imituje interfejs serwisu Netflix. Strona ta zazwyczaj prosi o wprowadzenie danych logowania, takich jak adres e-mail i hasło. Użytkownicy, wierząc, że odnawiają dostęp do swojego konta, nieświadomie przekazują cyberprzestępcom swoje dane uwierzytelniające oraz dane osobowe.

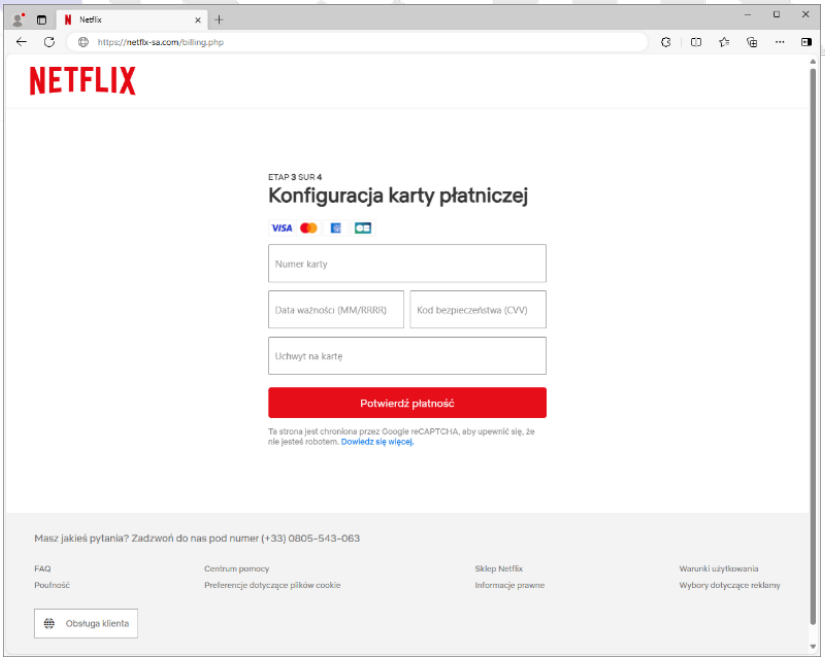


3. Fałszywa strona wyłudzająca dane logowania Netflix .



4. Fałszywa strona wyłudzająca dane osobowe.

Ostatecznym celem cyberprzestępców jest jednak uzyskanie danych kart płatniczych.



5. Fałszywa strona wyłudzająca dane karty płatniczej.

Opisywania kampania phishingowa wyróżnia się nie tylko globalnym zasięgiem, obejmującym rozmaite kraje z całego świata, ale również niezwykłą zdolnością do dostosowywania się i rozprzestrzeniania na masową skalę, szukając potencjalnych ofiar na wszystkich kontynentach. Przypadki użycia opisywanego scenariusza odnotowaliśmy w krajach takich jak: Niemcy, Hiszpania, Dania, Szwajcaria, Polska, Izrael, Katar, Bahrajn, Arabia Saudyjska, Chiny, Australia, Kolumbia, Brazylia oraz Republika Południowej Afryki.

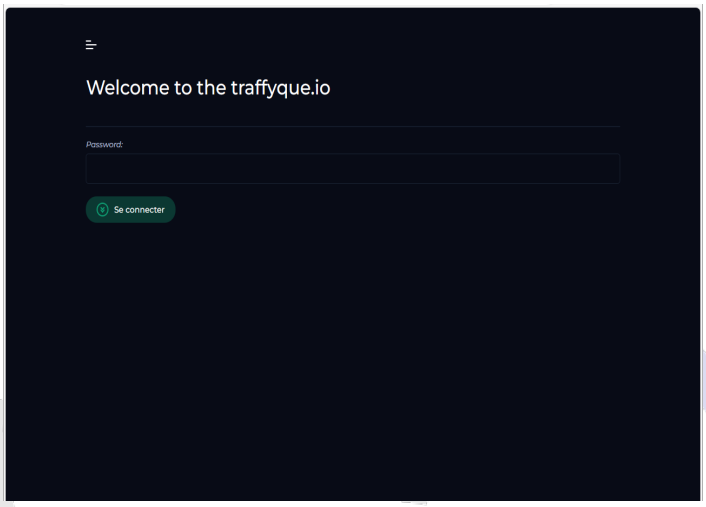
Ataki wykorzystują wizerunek różnych podmiotów - od usług streamingowych i firm kurierskich po operatorów telekomunikacyjnych - aby zwiększyć prawdopodobieństwo oszukania ofiar. Do oszustwa wykorzystywane są marki znane i zaufane przez szerokie grono odbiorców, co sprawia, że fałszywe komunikaty są bardziej przekonujące. **W Polsce zaobserwowaliśmy przypadki wykorzystania wizerunku podmiotów jak Netflix, DHL oraz Orange Polska.**

6. Ostrzeżenie CERT Orange odnośnie do opisywanej kampanii.
Źródło:
https://twitter.com/CERT_OPL/status/1767183861379637476

7. Ostrzeżenie CERT Polska odnośnie opisywanej kampanii.
Źródło:
https://twitter.com/CERT_Polska/status/1767105435679510562

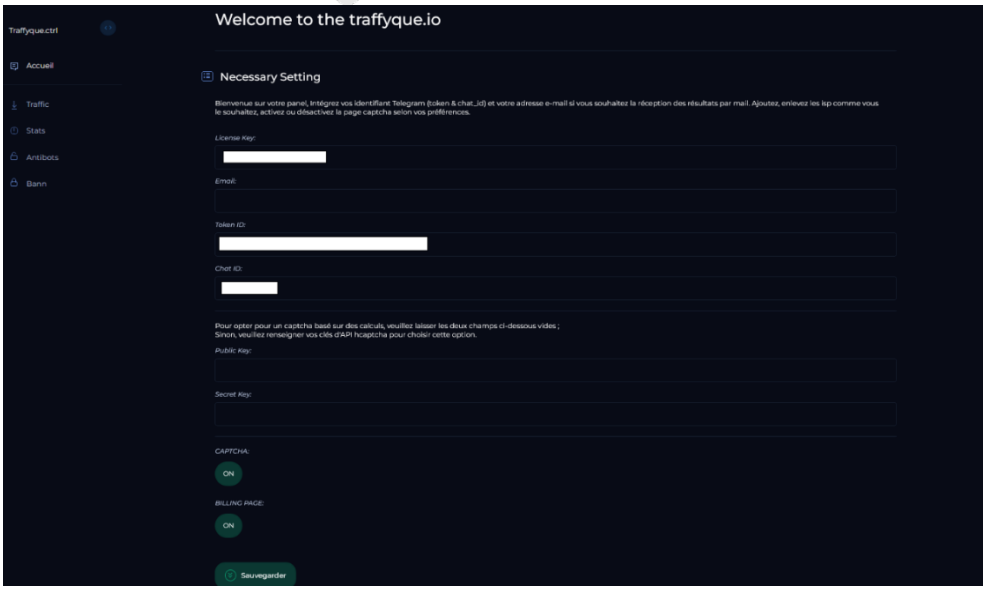
Panel zarządzania fałszywą stroną

Każda strona phishingowa w ramach kampanii jest wyposażona w prosty panel zarządzania, który zabezpieczony jest hasłem. Podstrona z panelem zawiera adres serwisu traffyque[.]io, funkcjonującego jako sklep internetowy w modelu Phishing as a Service (PaaS).



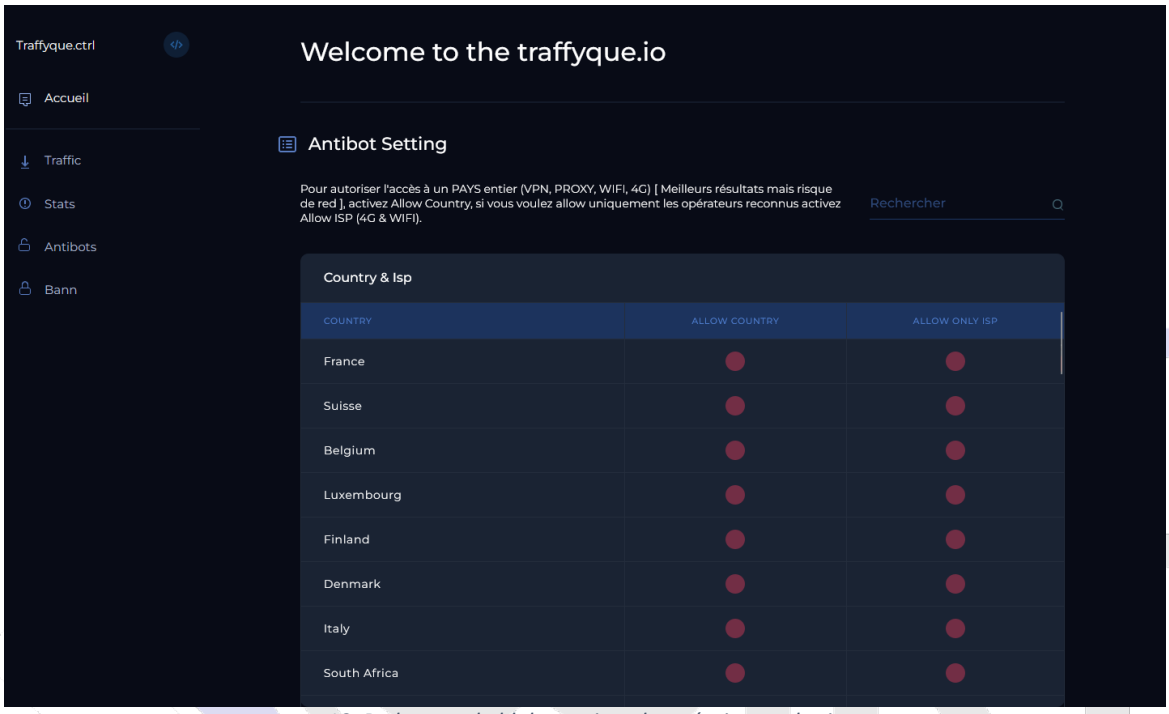
8. Panel zarządzania fałszywą stroną.

Po wprowadzeniu hasła cyberprzestępcy zyskują dostęp do funkcji panelu. Mogą oni ustawić specyficzny kanał na Telegramie oraz skonfigurować bota, który automatycznie będzie przekazywał zebrane dane, takie jak informacje o kartach kredytowych czy dane logowania ofiar. Wymagane jest również wprowadzenie klucza licencyjnego, zakupionego w serwisie traffyque[.]io.



9. Panel konfiguracyjny.

Jedną z cech tego systemu jest również zdolność do blokowania połączeń pochodzących z określonych krajów, co umożliwia przestępcom celowanie w użytkowników z wybranych regionów oraz minimalizuje ryzyko wykrycia przez organy ścigania z krajów, które są bardziej aktywne w walce z cyberprzestępczością



10. Podstrona do blokowania połączeń z innego kraju

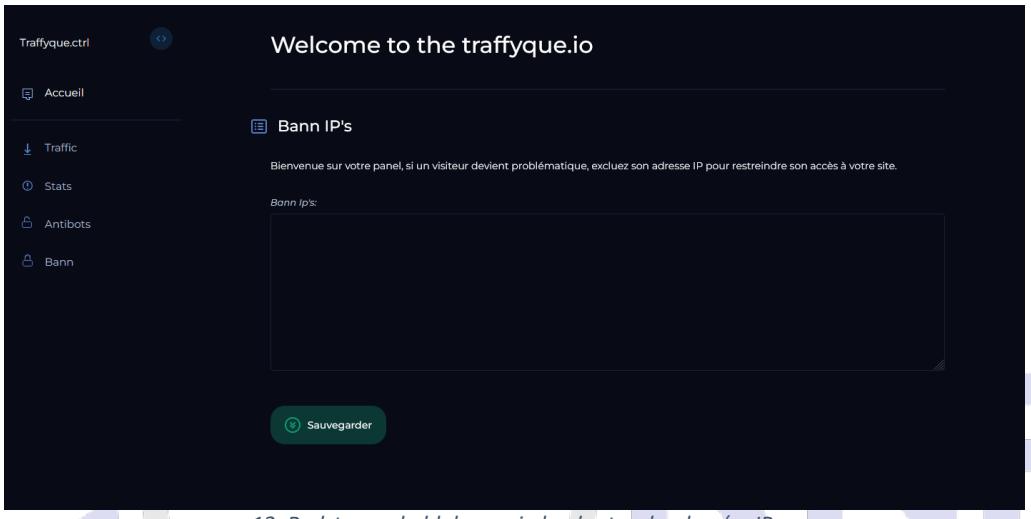
W przypadku próby uzyskania dostępu do strony phishingowej z kraju, który został zablokowany przez cyberprzestępców, użytkownikowi ukazuje się wiersz pochodzący z tomiku "Rewolucja" autorstwa francuskiego pisarza, Stephana Moysana.

```
Elle est le secret du bonheur,
Et son secret est le courage,
On en prend conscience dans l'angoisse,
Elle commence où l'ignorance finit.

Droit de chacun qui se limite au respect de l'autre,
Qui en prive l'homme est prisonnier de la haine
Des préjugés et de l'étroitesse d'esprit,
La liberté c'est de savoir danser avec ses chaines.
```

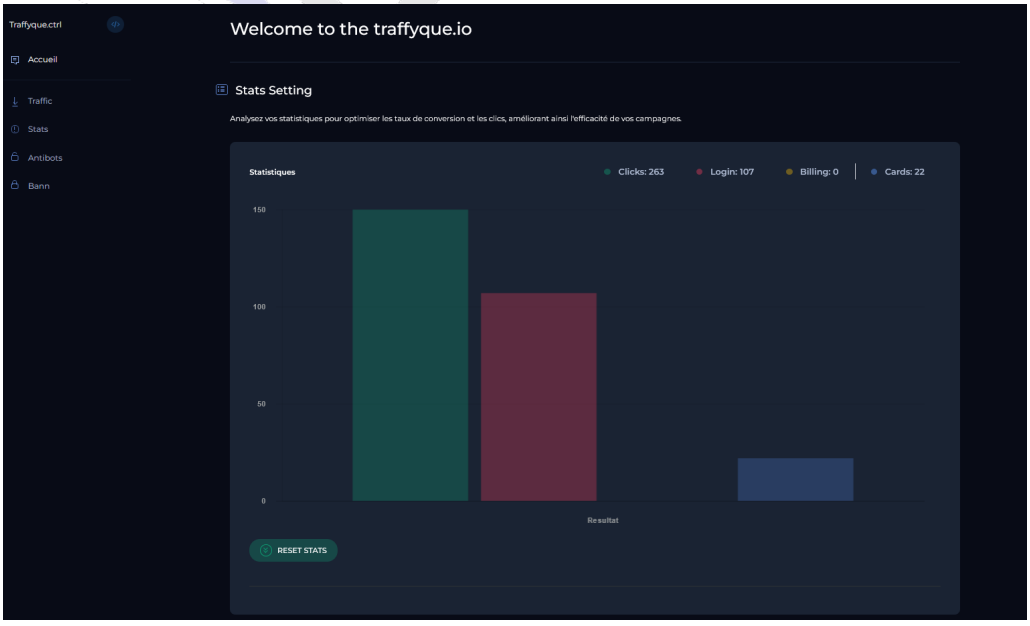
11. Zrzut ekranu wiersza umieszczonego na stronie.

Panel zarządzania stroną phishingową wyposażony jest również w funkcję, która umożliwia ręczne blokowanie konkretnych adresów IP próbujących nawiązać połączenie ze stroną. Ta funkcjonalność stanowi dodatkowy mechanizm obronny, mający na celu utrudnienie działań analityków cyberbezpieczeństwa w próbach analizy i identyfikacji złośliwej witryny.



12. Podstrona do blokowania konkretnych adresów IP.

Każda ze zidentyfikowanych stron phishingowych wyposażona jest w zaawansowane funkcje śledzenia statystyk. Te narzędzia umożliwiają atakującym monitorowanie kluczowych wskaźników efektywności kampanii, takich jak liczba kliknięć w linki, ilość prób logowania oraz liczba wprowadzonych danych kart płatniczych przez ofiary.



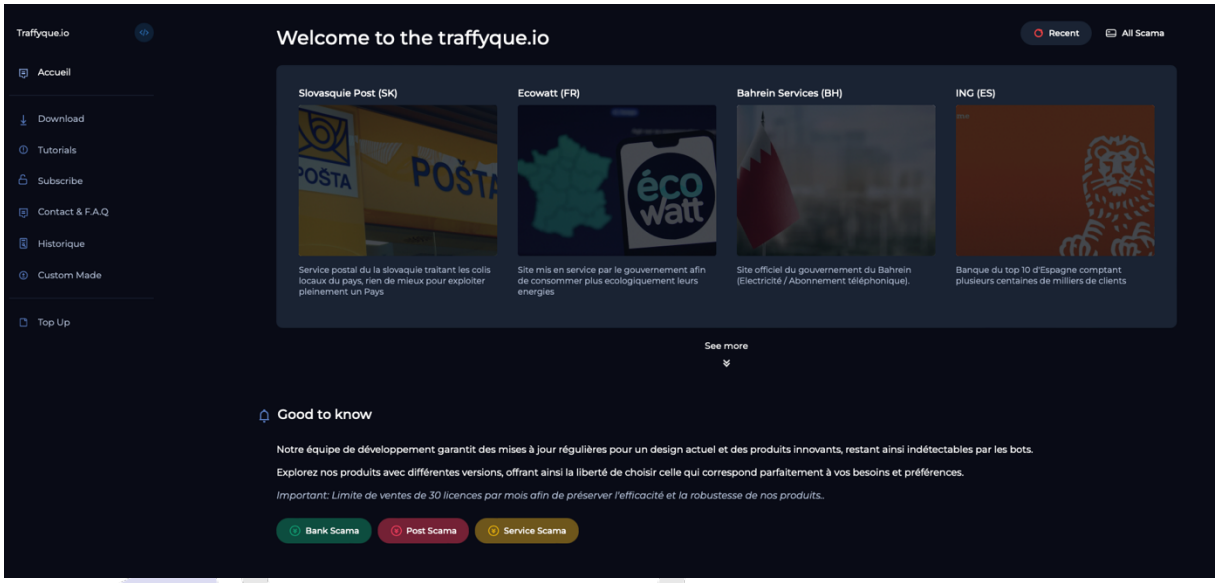
13. Podstrona ze statystykami fałszywej strony.

Gdy użytkownik wprowadzi swoje dane na fałszywej stronie, takie jak informacje logowania, dane osobowe czy numery kart płatniczych – te informacje są natychmiast przesyłane do przestępców za pośrednictwem Telegrama.

14. Wiadomość na kanale telegram.

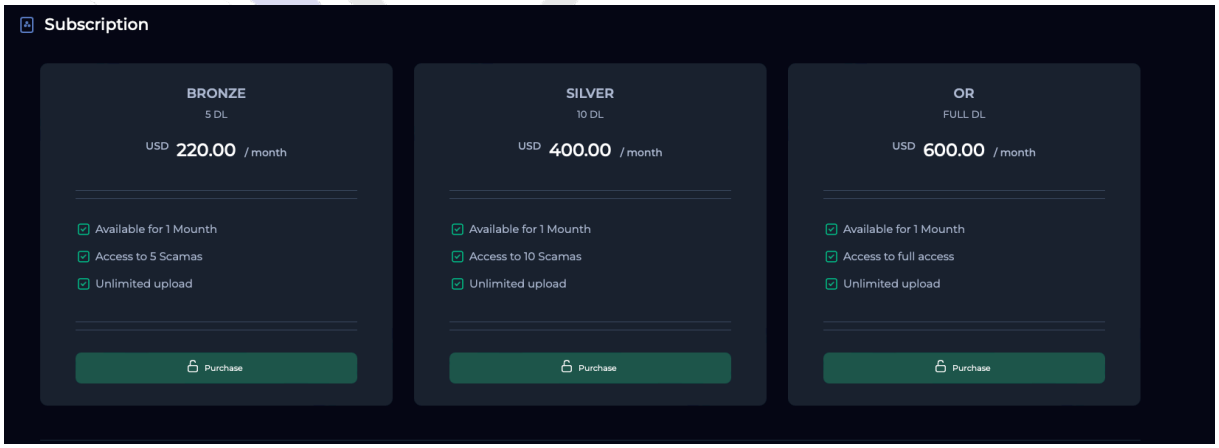
Profil cyberprzestępcy

Aktor do sprzedaży swoich usług - w tym wypadku paneli phishingowych - posługuje się domeną: traffyque[.]io.



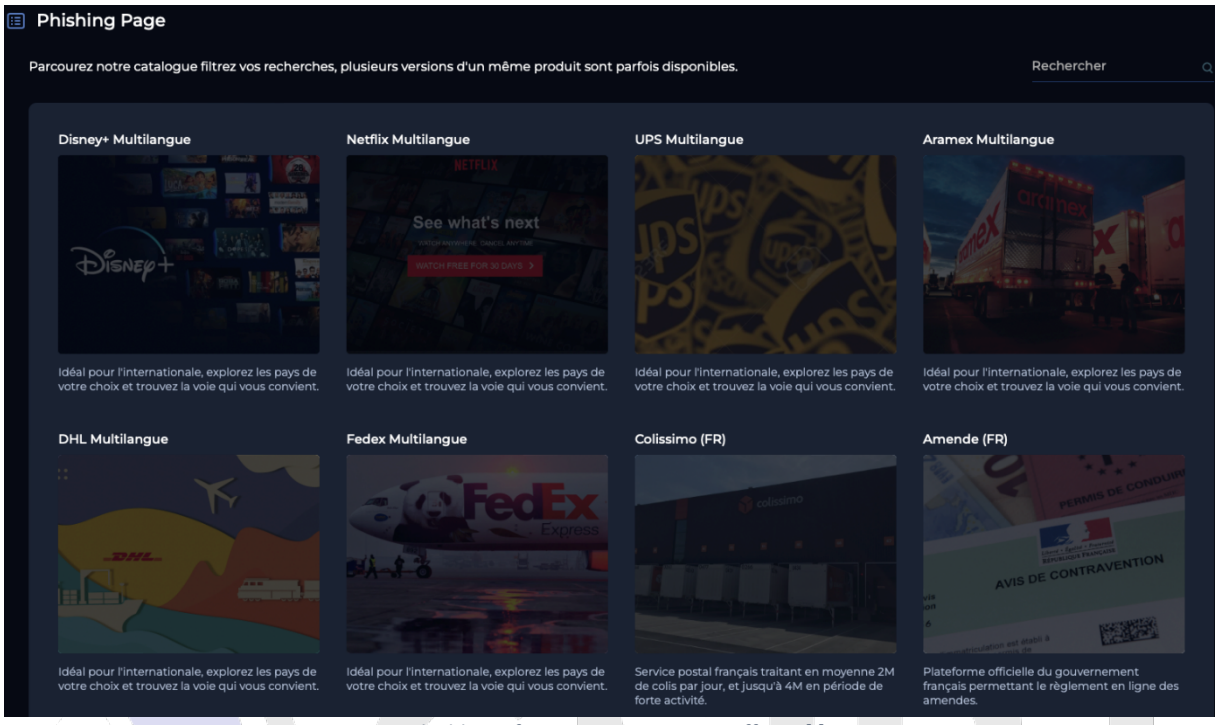
15. Strona traffyque[.]io

Na stronie internetowej, przestępca opublikował oferty sprzedaży paneli wraz z instrukcjami ich konfiguracji oraz cenami. Cena rośnie wraz z większymi możliwościami pakietu, który można zakupić.



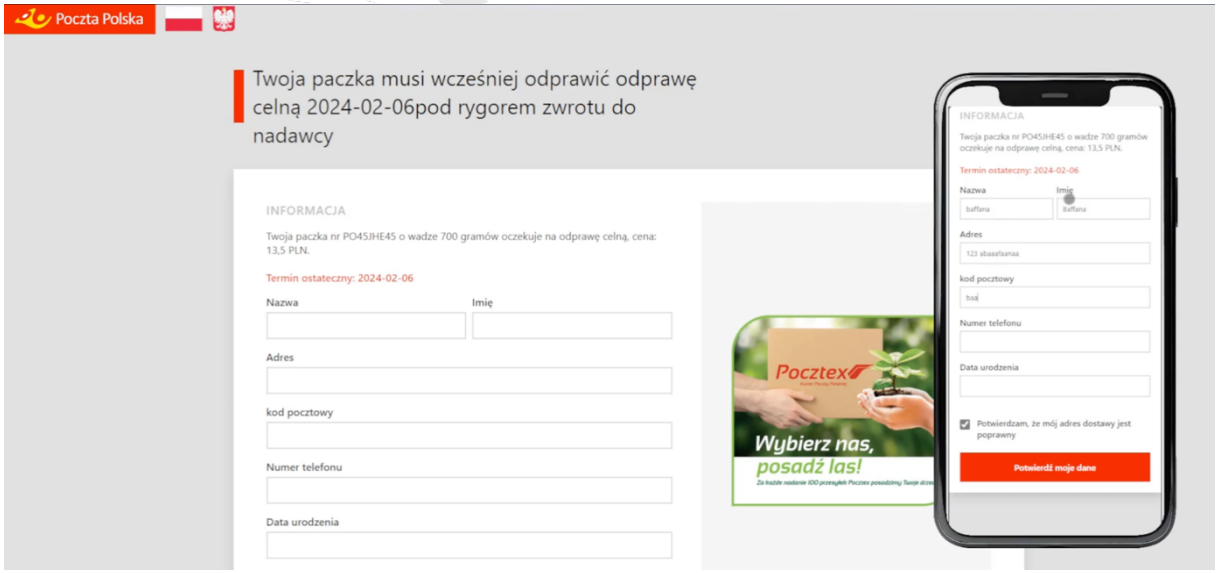
16. Oferta modelu Phishing as a Service oferowana na stronie traffyque[.]io.

W sekcji sprzedaży na ww. stronie internetowej, służącej do przeglądania oferty sprzedającego, możemy znaleźć całą gamę stron (52 skrypty phishingowe), które są już gotowe do zakupu oraz działania w charakterze przestępczym – phishingu.



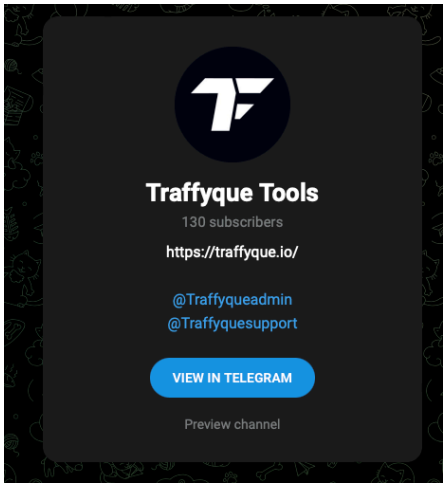
17. Phishkity oferowane na stronie traffyque[.]io.

Do każdej oferty fałszywej strony, jest podpięty film, który pokazuje działanie skryptu phishingowego.



18. Przykład phishkitu imitującego stronę Poczy Polskie.j Phishkity oferowanego na stronie traffyque[.]io.

Na stronie aktora, po kliknięciu w zakładkę kontakt, jesteśmy przekierowani do domeny Telegram, gdzie możemy dołączyć do kanału należącego do przestępcy.

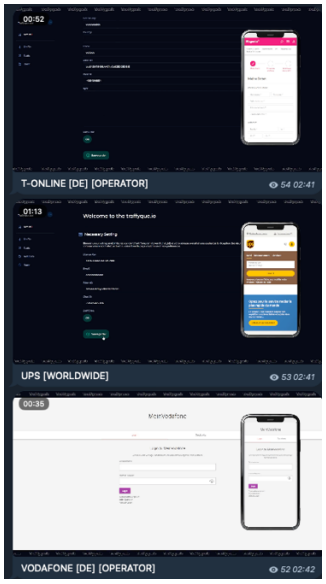


19. Kanał Telegram autora serwisu.

Do sprzedawcy skryptów phishingowych należy sześć kanałów Telegram:
1) **Traffyque** – kanał główny/oficjalny;
2) **Traffyque Tools** – prezentowane są na nim najnowsze skrypty phishingowe;
3) **TRAFFYQUE VOUCHES** – recenzje skryptów od kupujących wraz z zarobkami;
4) **Traffyque MEDIA** – publikowane są na nim filmy ze skryptami;
5) **Traffyque Admin** – kontakt do właściciela sklepu ze skryptami;
6) **Traffyque Support** – pomoc ze strony sprzedającego np. w konfiguracji skryptów;

Przykładowe zrzuty ekranu z kanałów Telegram:

20. Oferta umieszona na kanale telegram.

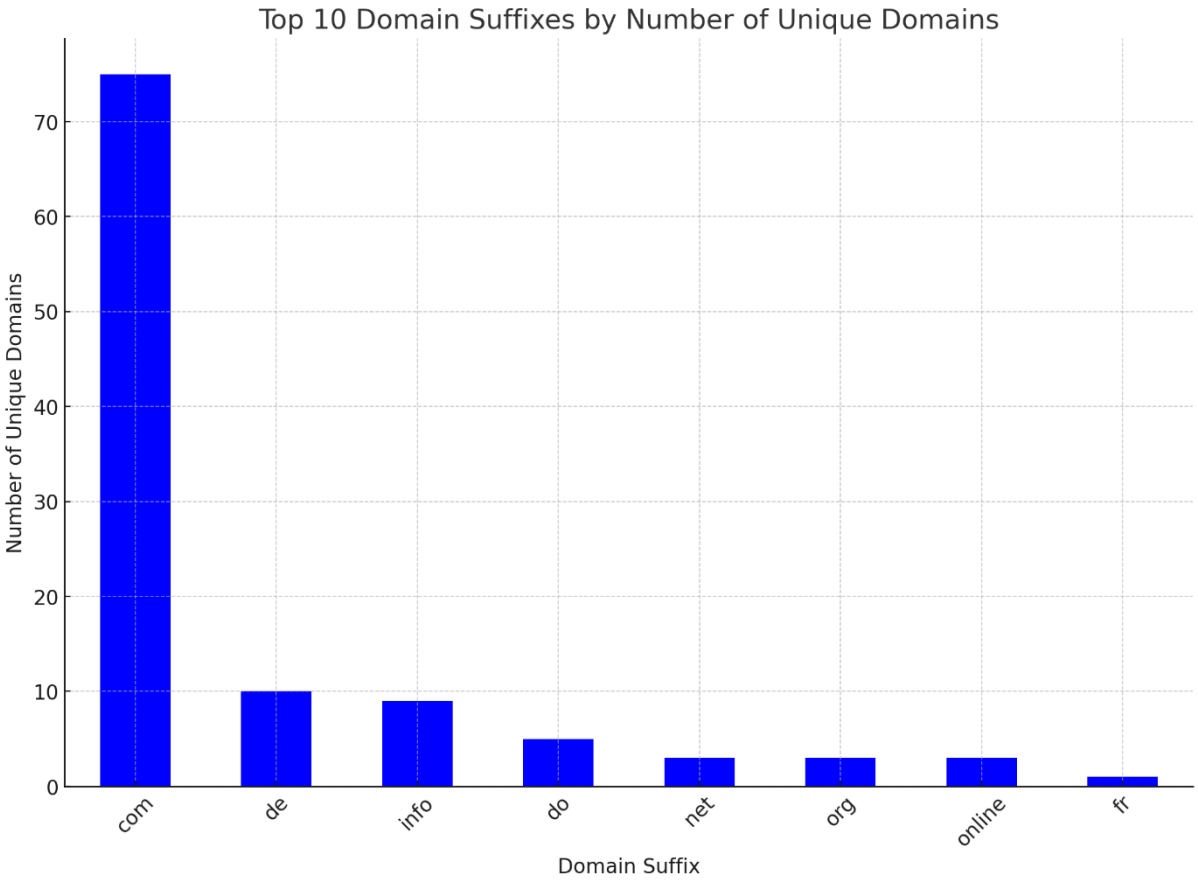


21. Przykłady oferowanych phishkitów.

Infrastruktura przestępców

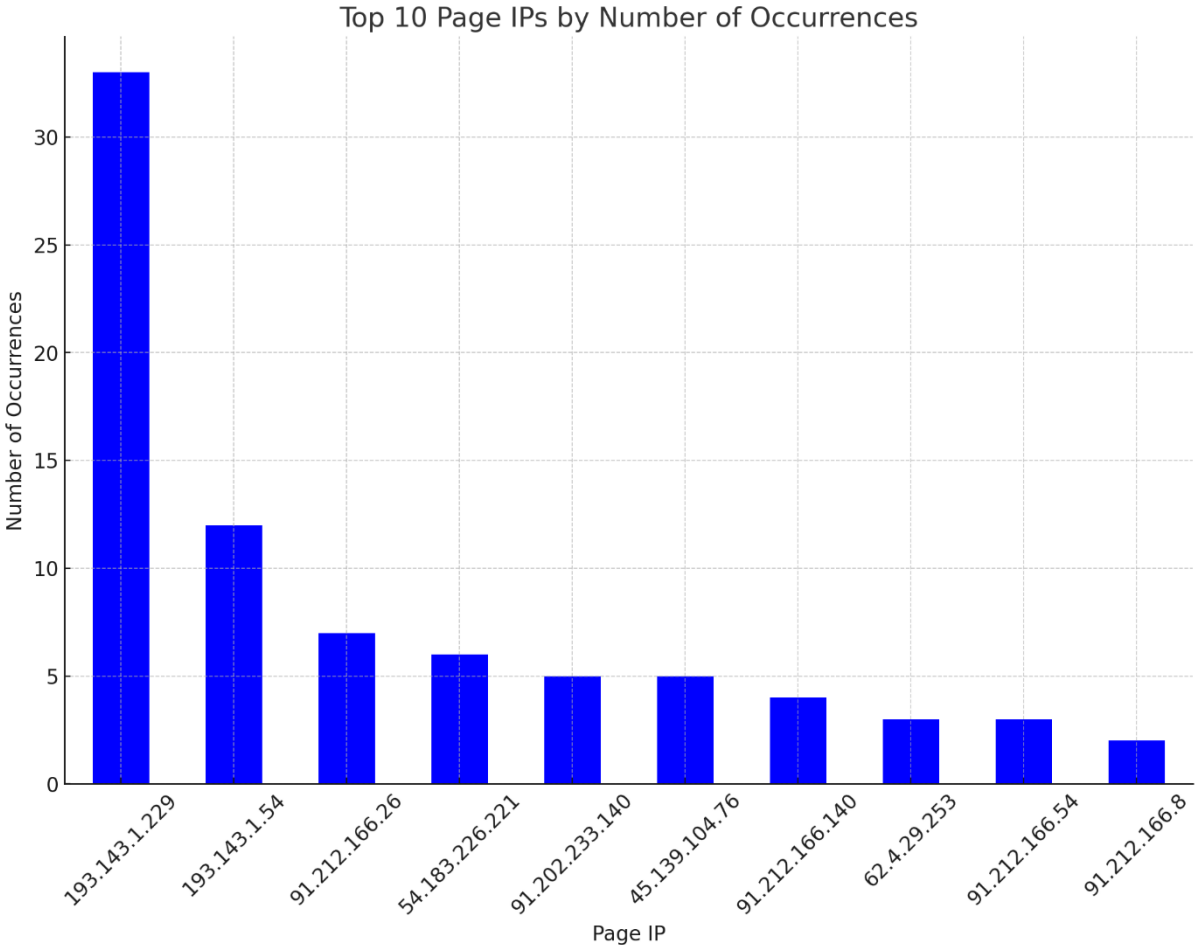
Infrastruktura wykorzystywana przez cyberprzestępców korzysta z wielu różnorodnych domen oraz adresów IP, na którą składa się 27 unikalnych adresów IP, 109 unikalnych domen oraz 12 unikalnych nazw organizacji AS.

Dominującym TLD wśród wykorzystywanych domen jest „.com”, który występuje 74 razy. Po nim, najczęściej używane TLD to „.de”, „.info” oraz „.do”.



Wykres 1. Top 10 domen najwyższego poziomu użytych w kampanii.

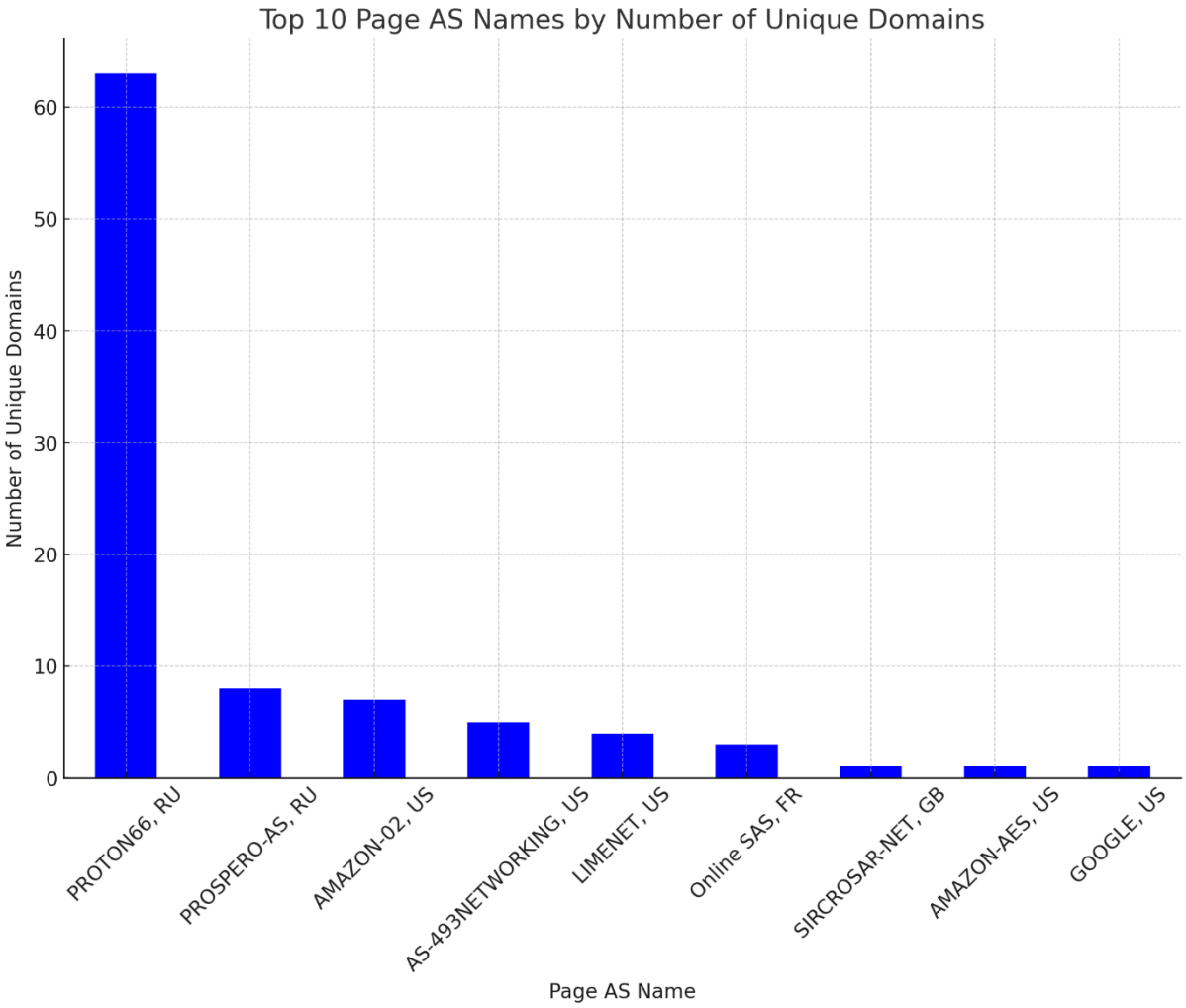
Przeważającym adresem IP domen jest 193.143.1.229, który jest powiązany z autonomicznym systemem o nazwie "PROTON66". Dwa kolejne najczęściej używane adresy to 193.143.77.54 oraz 91.212.166.26. Wszystkie trzy adresy IP należą do tego samego systemu autonomicznego.



Wykres 2. Top 10 wykorzystywanych adresów IP.

Proton66 (AS198953) jest dostawcą usług hostingowych z Rosji. Zarządza siecią z 1,280 adresami IPv4, nie posiadając adresów IPv6. System ten został przydzielony 6 kwietnia 2023 r. i ostatnio zaktualizowany 24 listopada 2023 r. Współpracuje z kilkoma dostawcami usług internetowych dla łączności sieciowej i jest zarejestrowany w bazie danych RIPE. Proton66 hostuje znaczną liczbę domen, w sumie 1,571 w swoim zakresie IP.

'45.134.26.0/24',	'45.135.232.0/24',
'45.140.17.0/24',	'45.155.205.0/24',
'91.212.166.0/24',	'193.143.1.0/24',



Wykres 3. Top 10 wykorzystywanych organizacji AS.

Adresy IP:

'193.143.1.229',	'193.143.1.131',
'91.212.166.140',	'193.143.1.54',
'45.139.104.76',	'91.212.166.26',
'91.212.166.54',	'91.202.233.140',
'54.183.226.221',	'62.4.29.253',
'91.212.166.8',	'91.202.233.159',
'94.156.8.153',	'62.210.144.206',
'91.202.233.132',	'34.203.223.94',
'193.143.1.186',	'193.143.1.229',

'91.92.252.51',	'94.156.67.159',
'145.14.157.109',	'91.215.85.5',
'91.92.244.98',	'3.143.115.180',
'94.156.69.164',	'91.212.166.8',
'35.186.223.180',	

Domeny:

'paketverzollung.com',	'fizetesaccount.com',
'abo-erneuerung.de',	'es-auth.do',
'netflxfi.com',	'netflx-sa.com',
'getyourflx.com',	'myups-switzerland.com',
'fizetesaccountsub.net',	'accountpago-flix.com',
'netflx-suomi.com',	'es.info.net.do',
'zollabfertigung-lieferung.de',	'abo-erneuern.de',
'accountflix-co.com',	'netflix-center.com',
'mysubscription-update.com',	'accountpago-co.com',
'account-flix-co.com',	'rinnovo-abbonamento.com',
'ayudacliente.org',	'spotify-abbuchung.de',
'netflx-au.com',	'clientfiixfr-app.com',
'account-nflix-co.com',	'spotify-rechnungsstellung.com',
'clientflixfrance-app.com',	'abozahlung.com',
'fizetesaccountflix.net',	'help-subscription.info',
'fizetesaccount-hu.com',	'account-ch.info',
'dhl-log.info',	'abonnement-regularisation.com',
'souscription-abonnement.online',	'rappel-societegen.org',
'setup-renewacc.com',	'renewapp-fiix.com',
'aboerneuerung.com',	'my.net-acces.com',
'defectopago-ntx-co.info',	'clientaides-app.com',
'abo-zahlung.de',	'www.fizetesaccount.com',
'www.mysubscription-update.com',	'fizetesaccount.net',
'procedure-securisation.com',	'suscripcion-actualizada.com',
'disproempa.com',	'netflix-mise-a-jour-paiement.info',
'ayuda-suscripcion.com',	'www.account-nflix-co.com',
'netflx-poland.com',	'netflx-renwal.com',
'netflx-asia.com',	'upsswitzerland.com',
'fizetesaccountflix.com',	'netflxcolombia.com',

'www.lieferung-dhl-tracking.de',	'netflixbahrain.com',
'ntx-paiement-fr.info',	'abo-abgelaufen.de',
'client-orangelu.com',	'www.rappel-societegen.org',
'clientflix-frapp.com',	'netflx-za.com',
'subscriptionsaccountflix-hu.com',	'refusalrenw.com',
'suivi-expeditioncolissimo.info',	'abos-zahlung.de',
'netflxqa.com',	'ntx-log.com',
'mynetflix-customer.com',	'netflxco.com',
'netflixpoland.com',	'account-hu.com',
'dan-denkmal.s3-website.eu-central-1.amazonaws.com',	'upsdenmark.com',
'netflxbills.com',	'membership-renw.com',
'abo-unterbrochen.de',	'pl-netflx.com',
'abonnement-verlenging.com',	'parcel-trackshipment.com',
'paiement-abonnement.info',	'netflx-il.com',
'netflx-qa.com',	'netflx-souscription.com',
'netflxrenew.com',	'netfl-pomoc.com',
'review.do',	'servicenflixfr-app.com',
'marqueepoque.s3-website.eu-central-1.amazonaws.com',	'rappel-suspension.online',
'account-co.com',	'renewal-subs.com',
'servicentflixfr-app.com',	'net-app.do',
'netfl-support-portal.com',	'mynetflixbahrain.com',
'odnowienie-linii.com',	'zahlung-verlangerung.de',
'netflx-pago.com',	'france-identites.fr',
'clientsaide-fr.info',	'rappel-souscription.online',
'approfile-updater.com',	'enel-br.com',
'netflx.sld.do',	

Organizacje AS:

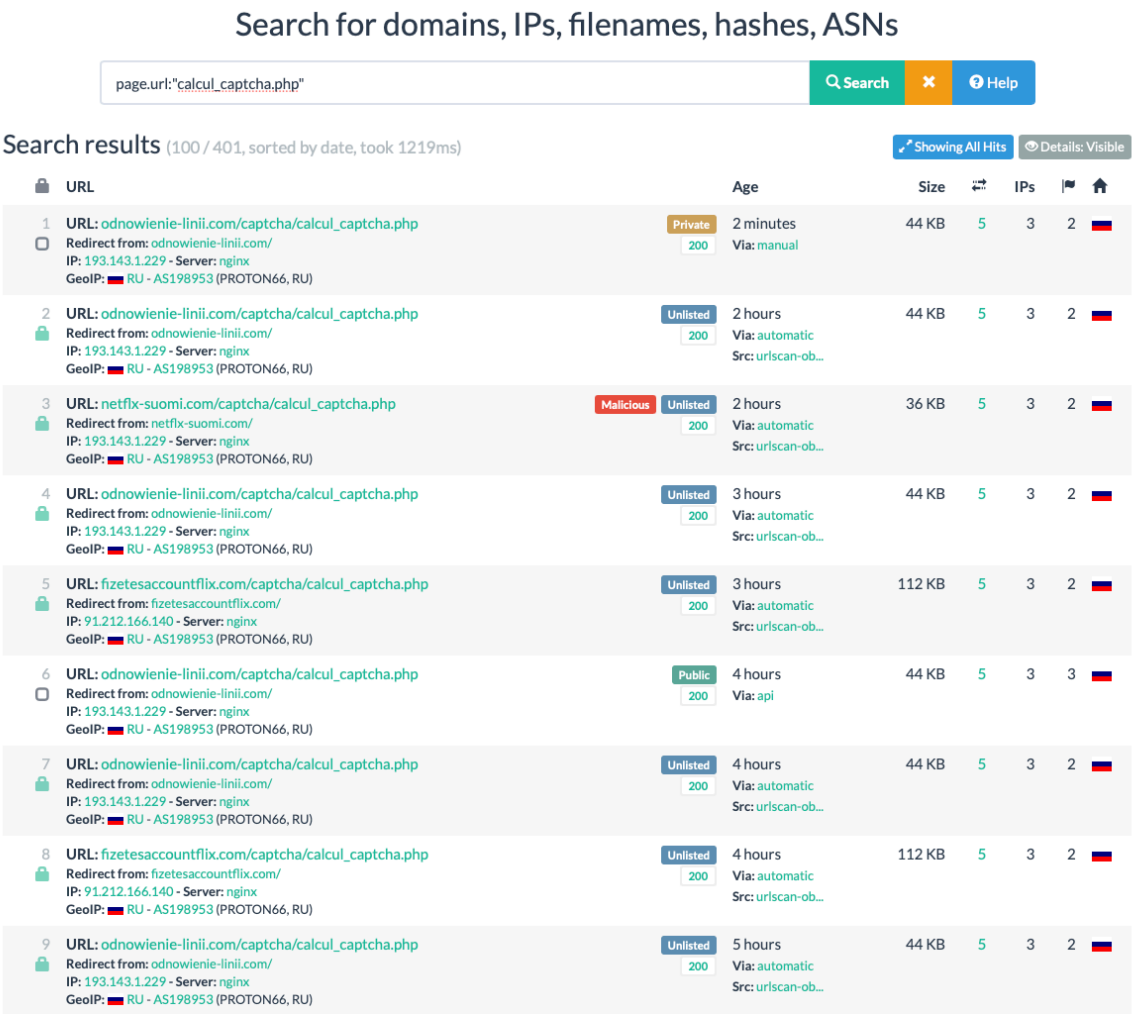
'PROTON66, RU',	'AS-493NETWORKING, US',
'PROSPERO-AS, RU',	'AMAZON-02, US',
'Online SAS, FR',	'SIRCROSAR-NET, GB',
'AMAZON-AES, US',	'LIMENET, US',
'AS-HOSTINGER, CY',	'AMAZON-02, US',
'Online SAS, FR',	'GOOGLE, US',

Szukanie infrastruktury cyberprzestępców

Przed wejściem na fałszywą stronę, zawsze zostaje nam wyświetlona weryfikacja captcha. Dzięki czemu, możemy śledzić oszukańcze strony za pomocą adresu URL.

Przykład:
https://FAŁSZYWASTRONA.PL/captcha/calcul_captcha.php

Taką możliwość daje nam na przykład serwis urlscan.io:



22. Przykładowe zapytanie na portalu shodan.io.

Użyte zapytanie:
`page.url:"captcha/calcul_captcha.php"`

Kolejną metodą, której wyniki są obiecujące to posłużenie się narzędziem Censys.io w dość specyficzny sposób, gdyż cyberprzestępca sprzedający swoje skrypty, zawsze pozostawia wiersz pochodzący z tomiku „Rewolucja” francuskiego autora Stephan’a Moysana:

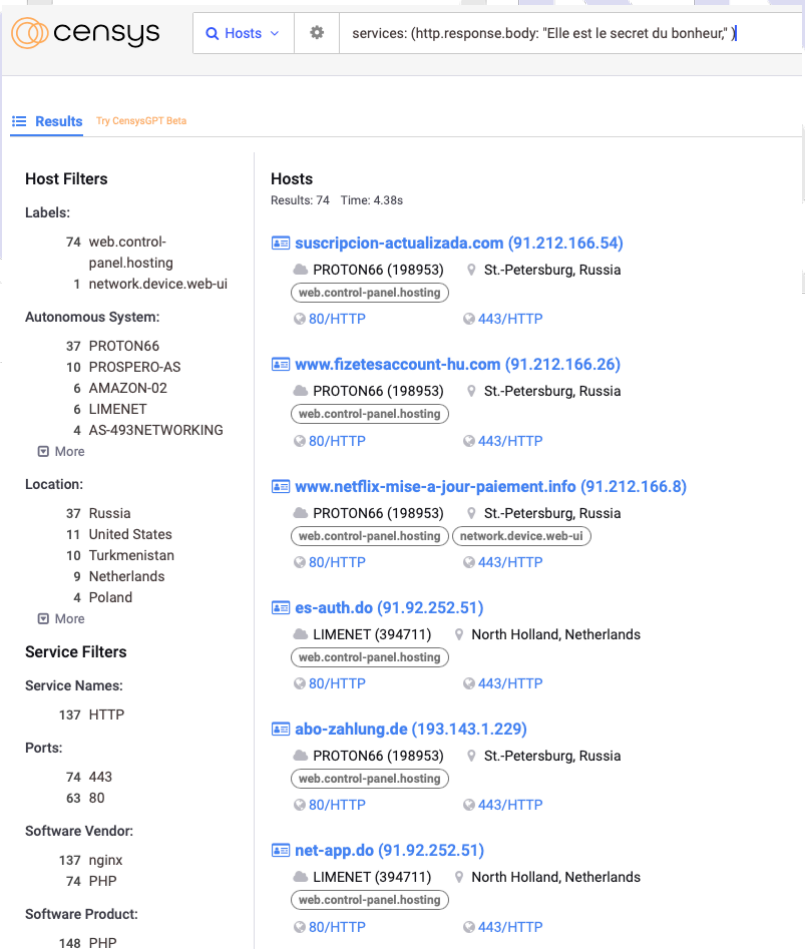
```
Elle est le secret du bonheur,
Et son secret est le courage,
On en prend conscience dans l'angoisse,
Elle commence où l'ignorance finit.

Droit de chacun qui se limite au respect de l'autre,
Qui en prive l'homme est prisonnier de la haine
Des préjugés et de l'étroitesse d'esprit,
La liberté c'est de savoir danser avec ses chaines.
```

23. Zrzut ekranu wiersza umieszczonego na stronie.

Aby znaleźć przestępczą infrastrukturę za pomocą poezji, wystarczy że stworzymy proste zapytanie:

```
services: (http.response.body: "Elle est le secret du bonheur")
```



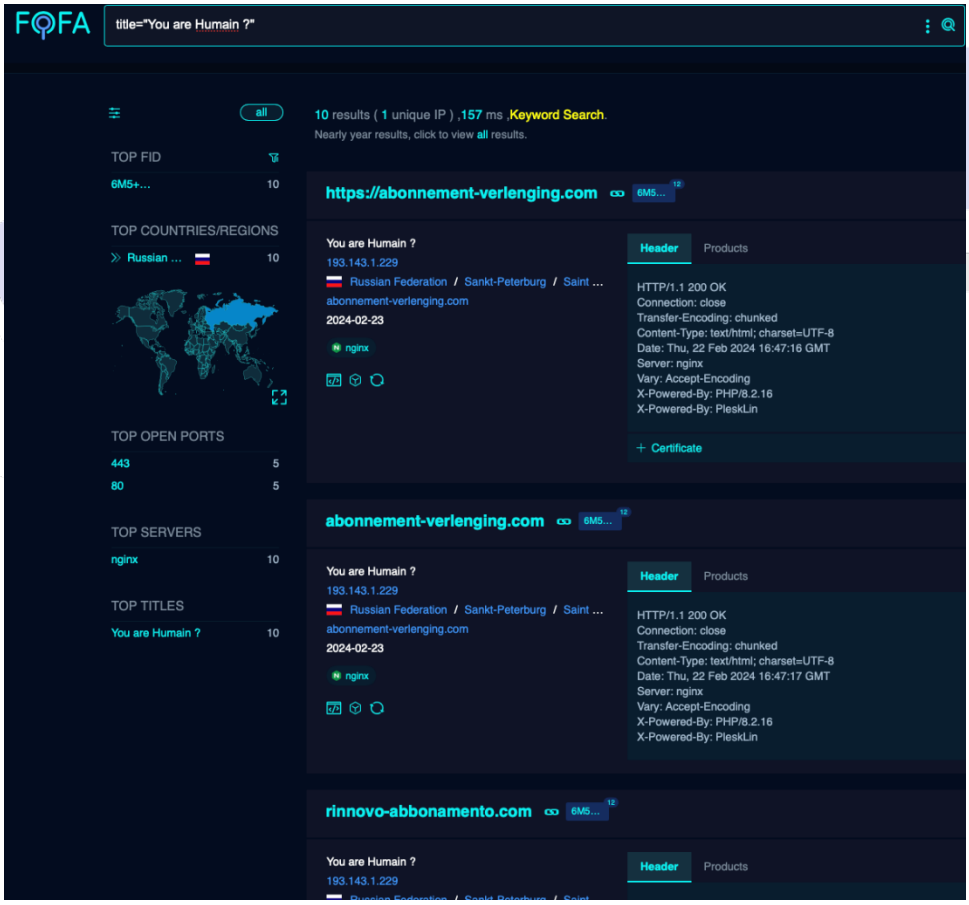
24. Przykładowe zapytanie na portalu search.censys.io.

Kolejną metodą, którą udało się zidentyfikować dzięki opieszałości cyberprzestępców jest utworzony przez nich tytuł strony, który wyświetla się podczas weryfikacji captcha.

Rekord ten, nosi nazwę:
Title: You are Humain ?

Na pierwszy rzut oka widać, że doszło do literówki i zamiast „Human” przestępca użył słowa „Humain”, dzięki czemu skuteczność wyszukiwania z pomocą tego prostego błędu znacznie się zwiększa.

W tym przypadku zostało użyte narzędzie FOFA info:



25. Przykładowe zapytanie na portalu fofa.info.

Wykorzystane zapytanie:
`title=”You are Humain ?”`

Podsumowanie

W dzisiejszych czasach, aby przeprowadzić skuteczny atak phishingowy, nie jest już wymagana zaawansowana wiedza techniczna. Narzędzia i infrastruktura niezbędne do wyłudzenia danych są dostępne na wyciągnięcie ręki, oferowane przez usługi Phishing as a Service z prostotą obsługi, która zmienia złożone schematy ataków w procesy "plug-and-play". To przypomnienie o tym, że zrozumienie i rozpoznawanie taktyk wykorzystywanych przez przestępców stanowi fundament budowania efektywnej linii obrony.

Czujność, edukacja i współpraca są niezbędne na wszystkich szczeblach społeczności cyfrowej, aby nadążać za ciągle ewoluującymi zagrożeniami. Zachęcamy do aktywnego śledzenia kont CSIRT KNF na portalu X, LinkedInie oraz Facebooku, gdzie regularnie informujemy o nowych metodach działania oszustów i sposobach ochrony przed nimi.