RIFFSEC

riffsec.com

RIFFSEC Report

Fałszywe inwestycje w sieci.

Schemat działania i zaplecze przestępcze.

Marzec 2026

Wstęp

Fałszywe inwestycje to jeden z najpowszechniejszych schematów oszustw finansowych w sieci. Przestępcy budują wiarygodną narrację inwestycyjną i stopniowo zdobywają zaufanie ofiary, by skłonić ją do przekazywania środków. Proces ten rzadko ma charakter jednorazowy. Trwa tygodnie lub miesiące, w trakcie których ofiara jest przekonywana o wysokiej skuteczności rzekomej inwestycji i czekających ponadprzeciętnych zyskach.

Schemat łączy reklamy w mediach społecznościowych z psychologiczną presją. Proceder często nie kończy się na pierwszej stracie. Ofiary są atakowane ponownie przez osoby podszywające się pod instytucje finansowe, kancelarie prawne lub firmy odzyskujące środki, które wyłudzają kolejne pieniądze pod pretekstem pomocy.

Rzeczywistą skalę strat trudno oszacować. Wiele osób nie zgłasza przestępstwa ze wstydu lub obawy przed oceną, zwłaszcza gdy dały się oszukać dwukrotnie. **Pewien obraz sytuacji daje sprawa rozbita przez CBZC Kraków we współpracy z oddziałami w Gorzowie i Radomiu: śledztwo objęło 7 fałszywych platform inwestycyjnych, zabezpieczono mienie o wartości 5 mln zł (kryptowaluty, samochody, kosztowności) oraz dodatkowe aktywa kryptowalutowe wyceniane na ponad 5 mln dolarów.** Warto podkreślić, że była to jedna z wielu tego typu grup, niekoniecznie należąca do najbardziej dochodowych.

Fałszywe inwestycje to działalność zorganizowanych grup przestępczych z wyraźnym podziałem ról. Od tworzenia reklam i stron, przez pozyskiwanie danych kontaktowych i prowadzenie rozmów z ofiarami, po obsługę przepływów finansowych. Taka struktura pozwala działać na dużą skalę, jednocześnie utrudniając identyfikację rzeczywistych sprawców. Zapraszamy do zapoznania się z tymi schematami, aby lepie je zrozumieć.

Autorzy raportu,
Agata Ślusarek, Adam Lange

Tomasz Jaroszek

Edukator finansowy, prezes Fundacji
na rzecz Edukacji Ekonomicznej Polaków

Między innymi dzięki sztucznej inteligencji, oszukiwanie nigdy nie było tak proste.
Piszę to jako osoba zajmująca się edukacją finansową, która od wielu lat pokazuje przeróżne zagrożenia związane m.in. z bezpieczeństwem naszych pieniędzy. Nie tylko widzę rosnącą potrzebę mówienia o tym temacie ze strony konsumentów i inwestorów, ale też palącą potrzebę mówienia o tym z poziomu bankowości i rynku kapitałowego. Instytucje finansowe chowając się za tajemnicą bankową nie pokazują skali zjawiska, ale same cały czas inwestują w dodatkowe zabezpieczenia i zatrudniają ludzi w działach bezpieczeństwa. Jeśli w telewizji widzę warte miliony złotych reklamy banków mówiące o cyberbezpieczeństwie, to mam pewność, że skala zjawiska jest ogromna.

Rok temu pokazywałem na sali pełnej inwestorów deepfake, który sam zrobiłem z użyciem własnych materiałów video. Ostrzegałem, że za moment będziemy zalani falą takich produkcji i coraz częściej oszuści będą sięgać nie tylko po wizerunek sportowców, aktorów czy polityków, ale właśnie specjalistów zajmujących się finansami. Od tamtego czasu zgłosiłem niemal 100 swoich sobowtórów z różnych kanałów social media, a raz znalazłem nawet swoje nazwisko piramidzie finansowej zarejestrowanej na dalekich wyspach południowej Azji, gdzie zasiadam rzekomo w „Radzie Dyrektorów” (wraz z innymi kolegami z Polski, których wizerunki skradziono).

Takich oszustw będzie tylko więcej. Samo zjawisko „fałszywych inwestycji” wpływa bardzo negatywnie na cały obraz polskiego rynku kapitałowego. W ubiegłym roku nasze indeksy giełdowe zyskały ponad 45%, to jeden z najlepszych wyników na świecie. Jednak dla wielu Polaków rynek kapitałowy wydaje się czymś trudnym i wręcz niebezpiecznym. Zamiast skupiać się na edukacji dotyczącej inwestowania długoterminowego, priorytetem sektora finansowego stała się nauka jak odróżnić fałszywe inwestycje. Jesteśmy krajem, który jeszcze nie zdążył wyedukować solidnie pokolenia inwestorów, a już musi walczyć z masowymi oszustwami.

Poniższy raport pozwala nam zobaczyć dwie warstwy tego zjawiska. Pierwszą warstwę znam doskonale, bo to proces oszukiwania konsumenta, który wpada w sidła wirtualnych oszustów. Widzę go niemal codziennie. Druga część raportu jest zarazem fascynująca i przerażająca, bo pokazuje jak działa i nieustannie rozwija się branża oszustów od środka. Możemy dosłownie zajrzeć na zaplecze tej działalności i nieco inaczej spojrzeć na skalę tego karygodnego przedsięwzięcia.

Cyberbezpieczeństwo to jak nauka samoobrony, tylko w realiach Internetu. Zachęcam do lektury, bo dzięki takiej wiedzy możemy lepiej poznać metody działania przeciwnika, na którego prędzej czy później trafimy w sieci.

Opis scenariusza

Schemat omawianego przestępstwa ma powtarzalny przebieg, który można podzielić na kilka następujących po sobie etapów. Choć poszczególne elementy mogą się różnić w zależności od grupy przestępczej lub wykorzystywanej platformy, ogólna logika działania pozostaje podobna.

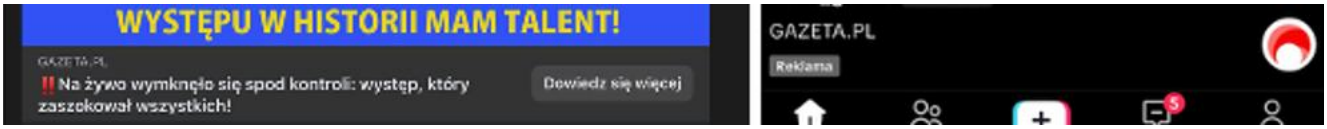
Etap pierwszy: reklamy w Internecie

Scenariusz zazwyczaj rozpoczyna się od prostej reklamy. Te „super oferty inwestycyjne" publikowane są w mediach społecznościowych głównie na portalu Facebook i TikTok, rzadziej, ale również na Instagramie, Twitterze (obecnie X), czy też jako reklamy w wyszukiwarce Google. Wybór miejsca publikacji, zależy od tego, gdzie atakujący uznają, że mają największe szanse dotarcia do wybranej grupy docelowej. W publikowanych reklamach oszuści korzystają z całej gamy róznych sztuczek socjotechnicznych, aby ich treści były jednocześnie wiarygodne i przyciągały uwagę odbiorcy. Te fałszywe publikacje mogą zawierać nagłówki sugerujące przełomową metodę inwestowania, historię szybkiego wzbogacenia się lub rekomendacje skradzionego wizerunku znanych osób ze świata biznesu i mediów. Stosunkowo często wykorzystywane są również nazwy rozpoznawalnych instytucji lub logotypy znanych marek, co ma zwiększyć wiarygodność przekazu.

Przykładowa reklama

Przykładowa reklama

Ważnym elementem tych materiałów jest obietnica wysokich i szybkich zysków przy jednoczesnym ograniczeniu lub braku ryzyka inwestycyjnego. Tego typu komunikaty są konstruowane w sposób, który ma wywołać poczucie wyjątkowej okazji oraz skłonić użytkownika do działania. Warto tez zwrócić uwagę na podpis towarzyszący publikacji.



Mechanizm podpisu

W tym przypadku przestępcy wykorzystali możliwości („feature, not a bug”), jakie daje Facebook w zakresie opisu reklamy oraz podpisu standardowego nagrania publikowanego na TikToku. Przestępcy umieszczają tam nazwy rzeczywistych, legalnie działających portali internetowych, co zwiększa wiarygodność treści reklamy. Jednocześnie atakujący starają się wzbudzić zainteresowanie publikowaną tematyką. Jednym z najczęściej wykorzystywanych motywów jest rzekomo ujawniany skandal.

> O ile w przypadku TikToka widoczność takich elementów wynika bezpośrednio ze sposobu działania platformy, o tyle w przypadku Facebooka trudno wskazać uzasadnienie dla tej funkcji z perspektywy użytkownika. Mechanizm ten pozwala na przykrycie faktycznego adresu strony oszukańczej zaufanym tekstem sugerującym legalny serwis. W praktyce użytkownik widzi np. „gazeta.pl”, podczas gdy po kliknięciu zostaje przekierowany na stronę zarządzaną przez przestępców.

Przykładowe reklamy

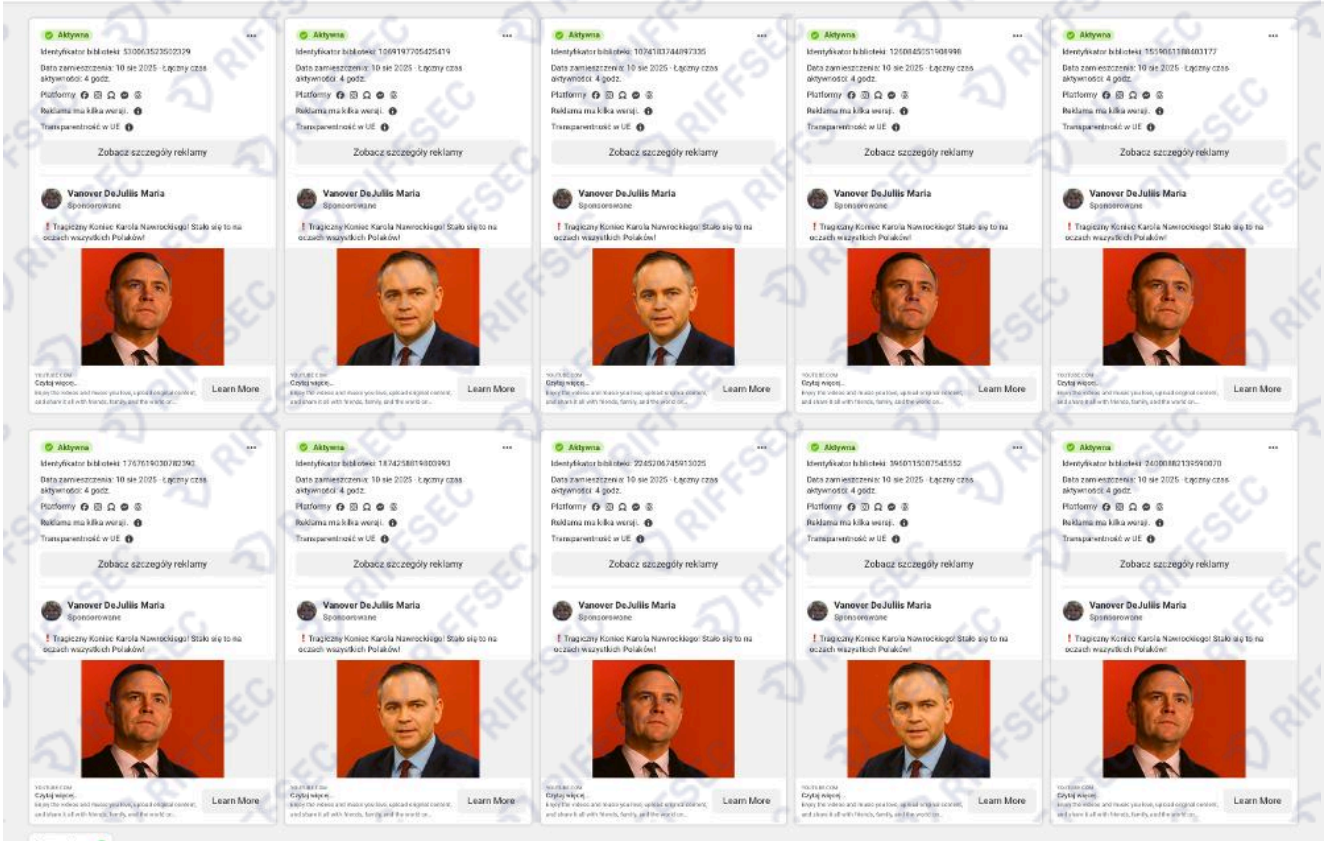
Przestępcy, dążąc do zwiększenia sensacyjności przekazu oraz przyciągnięcia uwagi odbiorcy, wykorzystują również motyw śmierci. Reklamy tego typu odwołują się do rzekomych testamentów lub nagłych zdarzeń losowych, mających wzbudzić silną reakcję emocjonalną i skłonić użytkownika do interakcji.

Przykładowa reklama

Przykładowa reklama

> Scenariusz fałszywych inwestycji nie jest problemem ograniczonym geograficznie. Zorganizowane, hierarchiczne grupy przestępcze prowadzą tego typu działania równolegle w wielu krajach. Większa skala bezpośrednio przekłada się na wyższe zyski grup przestępczych.

W Polsce przykładem wykorzystania bieżących wydarzeń były wybory prezydenckie. W krótkim czasie po ogłoszeniu wyników zaczęły pojawiać się reklamy sugerujące rzekomy skandal z udziałem prezydenta. Mechanizm ten opiera się na wykorzystaniu zwiększonej uwagi społecznej oraz emocjonalnego zaangażowania odbiorców. Schemat ten był wykorzystywany na dużą skalę, co potwierdza liczba opublikowanych reklam na Facebooku, wykorzystujących taką samą kreację. Poniższy zrzut ekranu przedstawia przykłady reklam wykorzystujących wizerunek prezydenta wraz z identycznym opisem.



Przykładadowe reklamy wykorzystujące ten sam motyw

Kilkadziesiąt reklam aktywnych jednocześnie na Facebooku. Jednocześnie analiza kont reklamowych wskazuje, że kampanie te są prowadzone równolegle na wielu rynkach. Z jednego konta publikowane są reklamy w różnych językach oraz wariantach scenariusza, co potwierdza ich międzynarodowy charakter.

Jedno konto reklamowe – wiele języków i rynków

Przestępcy coraz częściej sięgają również po technologię deepfake. Tworzą materiały wideo wykorzystujące wizerunek oraz ton głosu znanych osób, aby także w ten sposób zwiększyć wiarygodność przekazu. Rozwój narzędzi sztucznej inteligencji odczuwalny jest w wyraźnym postępie jakości materiałów deepfake przygotowywanych przez przestępców na przestrzeni kolejnych miesięcy. Podobnie jak wcześniej, materiały powstają w różnych językach, w zależności od potrzeb atakujących.

Wykorzystanie technologii deepfake nie jest obecnie warunkiem skuteczności kampanii. Statyczne reklamy nadal zapewniają atakującym wysoki zwrot. Mimo to obserwowany jest bardzo dynamiczny rozwój tego obszaru.

Przykładowe nagrania deepfake

NYHET: *Sannheten er nå avslørt, og vi var ikke klare for den.*
→ **WIADOMOŚĆ:** „Prawda została teraz ujawniona i nie byliśmy na nią gotowi."

EKSKLUSIVT: DETALJER FRA VITNEFØRINGEN.
→ **EKSKLUZYWNIE: szczegóły z zeznań świadków.**

Tłumaczenie

Przykładowe nagrania deepfake

„Tylko 6% Greków o tym wie.
Zarabiaj ponad 10 000 € miesięcznie — gwarantowane."

Tłumaczenie

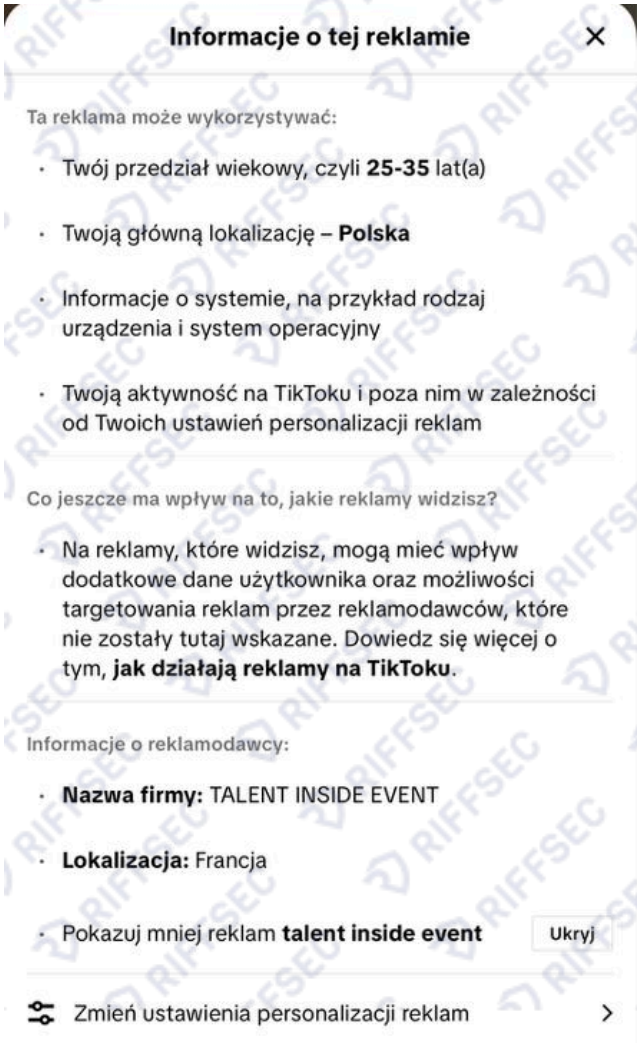
Agnieszka Gryszczyńska

Doktor habilitowany nauk prawnych, inżynier informatyk, profesor uczelni w Katedrze Prawa Informatycznego na Wydziale Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie

Zgodnie z rozporządzeniem 2024/1689 deepfake to wygenerowane przez AI lub zmanipulowane przez AI obrazy, treści dźwiękowe lub treści wideo, które przypominają istniejące osoby, przedmioty, miejsca, podmioty lub zdarzenia, które odbiorca mógłby niesłusznie uznać za autentyczne lub prawdziwe. Rozporządzenie to zobowiązuje wprawdzie podmioty stosujące system AI, który generuje deepfake do ujawniania, że treści te zostały sztucznie wygenerowane lub zmanipulowane, jednak z wiadomych względów obowiązku tego nie będą przestrzegali cyberprzestępcy wykorzystujący tą technologie dla osiągnięcia własnych, niezgodnych z prawem celów. Dodatkowo prawo polskie nie przewiduje przepisów penalizujących produkowanie czy rozpowszechnianie deepfake, a nie każde zmanipulowane obrazy, treści dźwiękowe lub treści wideo będą jednocześnie wyczerpywały znamiona przestępstwa kradzieży tożsamości, o którym mowa w art. 190a §2 k.k.

Warto również zwrócić uwagę, że atakujący ukierunkowują przekaz aby trafić do różnych grup wiekowych. Możemy znaleźć reklamy stricte wskazujące na chęć zainteresowania seniorów, ale widać także, że pozycjonują materiały do młodszych odbiorców, dobierając odpowiednią tematykę i scenariusz.

Przykładowe reklamy

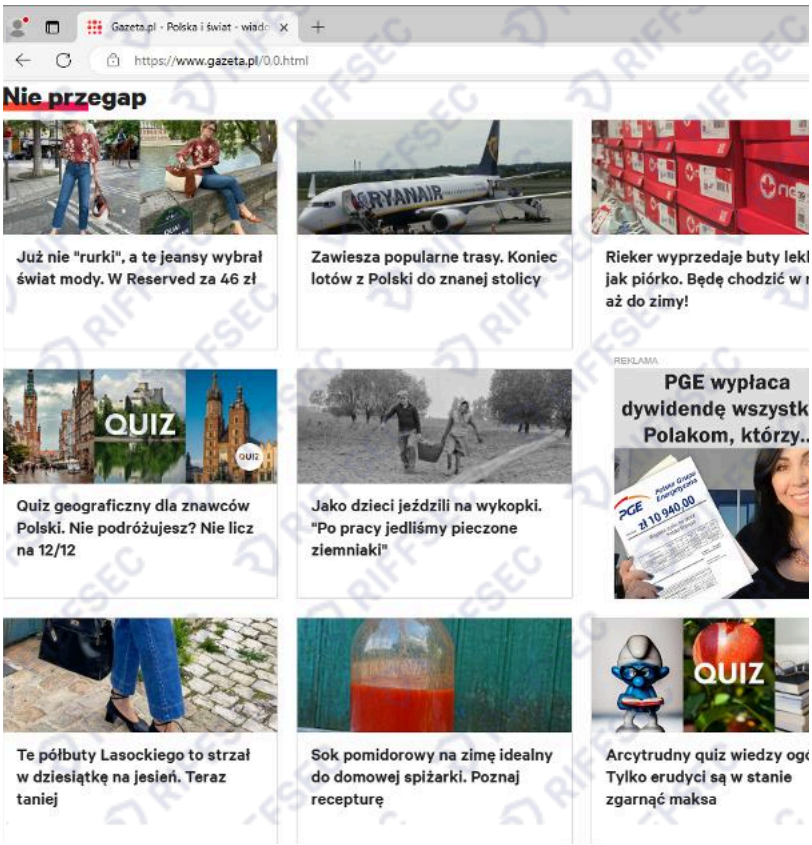


Szczegóły reklamy na TikTok'u

Reklamy w wyszukiwarce Google stanowią kolejny kanał wykorzystywany przez przestępców w schematach fałszywych inwestycji. Chętnie z nich korzystają, ponieważ pozwalają stosunkowo łatwo budować poczucie legalności oferowanej usługi. Fałszywe platformy inwestycyjne często pojawiają się wysoko w wynikach wyszukiwania, szczególnie w sytuacjach, gdy przestępcy podszywają się pod faktycznie istniejącą platformę inwestycyjną lub inną rozpoznawalną markę. Mechanizm działania wyszukiwarki powoduje, że płatne reklamy powiązane z określonymi słowami kluczowymi wyświetlają się na początku listy wyników wyszukiwania i choć są one oznaczone jako „reklama", wielu użytkowników nie zwraca na to uwagi, dodatkowo, fakt bycia reklamą w tej sytuacji nie powoduje poczucia niepokoju.

Reklamy wykupione w systemie Google wyświetlają się również na legalnych portalach internetowych w sekcjach oznaczonych jako „reklama". W praktyce często są one prezentowane w sposób zbliżony do standardowych artykułów publikowanych na danym portalu, przez co dla części użytkowników mogą wyglądać jak jeden z wielu materiałów redakcyjnych.

Poniżej przedstawiono przykładowy widok takiej reklamy z przeglądarki na komputerze oraz urządzanie mobilnego.



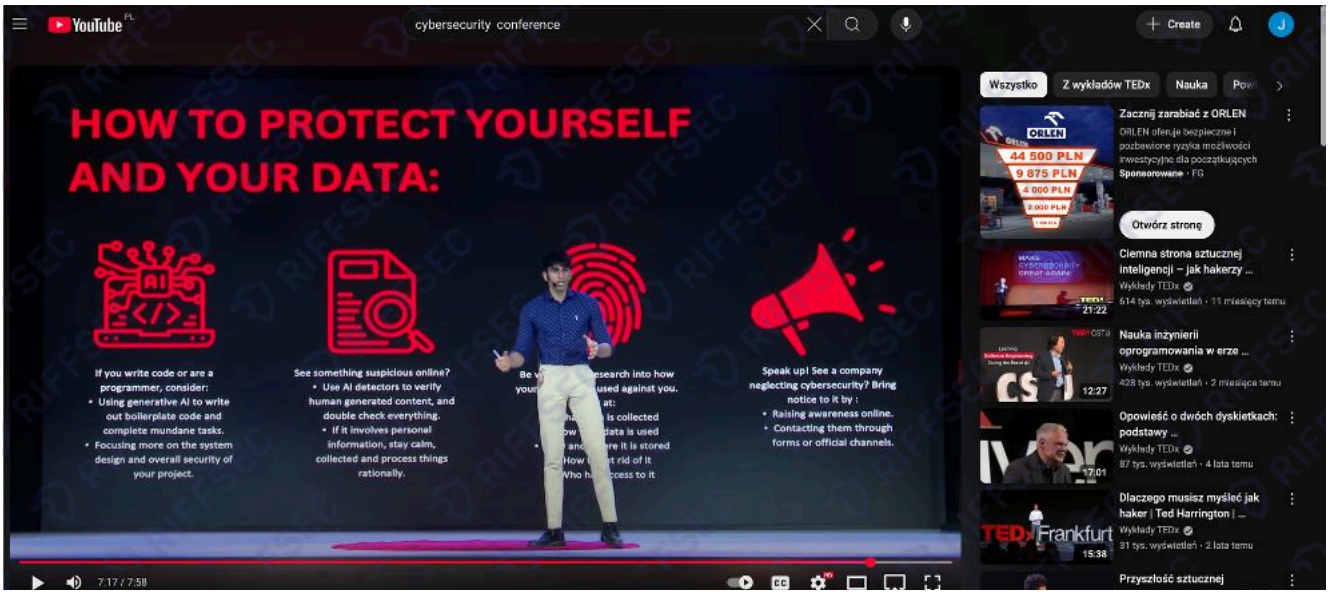
Widok reklamy Google z przeglądarki na komputerze

Widok reklamy z telefonu

Należy również zwrócić uwagę na sposób prezentacji takich treści na stronie. Dla niewprawnego użytkownika Internetu materiał ten może wyglądać jak standardowy artykuł publikowany na portalu, mimo że w rzeczywistości jest to płatna reklama.

> Portal, na którym wyświetlana jest reklama, nie ma bezpośredniego wpływu na jej treść, odpowiada za nią zewnętrzny dostawca reklamy (w tym wypadku Google). W ten sposób treści publikowane przez przestępców wyświetlane są w obrębie legalnych i rozpoznawalnych serwisów, co istotnie zwiększa skuteczność kampanii.

Reklamy w systemie Google wyświetlane są także na innych platformach internetowych. Przykładem może być YouTube, gdzie pojawiają się w dedykowanych przestrzeniach reklamowych na stronie.



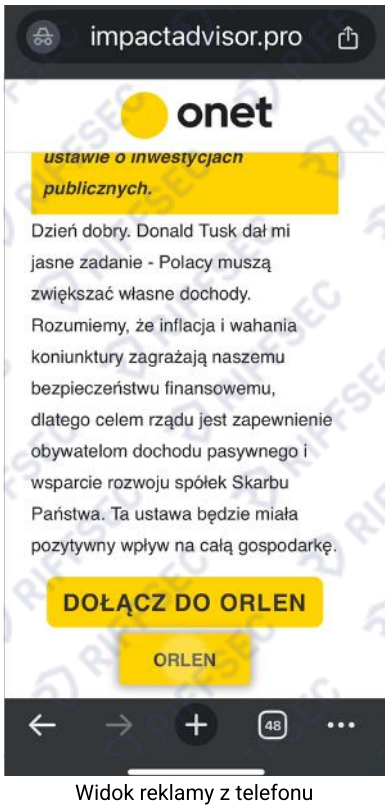
Widok reklamy Google na Youtube

Niezależnie od miejsca publikacji reklamy oraz zastosowanej formy (statycznej lub opartej na technologii deepfake), kluczowym celem przestępców jest skłonienie użytkownika do kliknięcia w link. To działanie stanowi punkt przejścia do kolejnego etapu schematu, którego celem jest pozyskanie danych kontaktowych użytkownika.

Etap drugi: formularz do wpisania danych

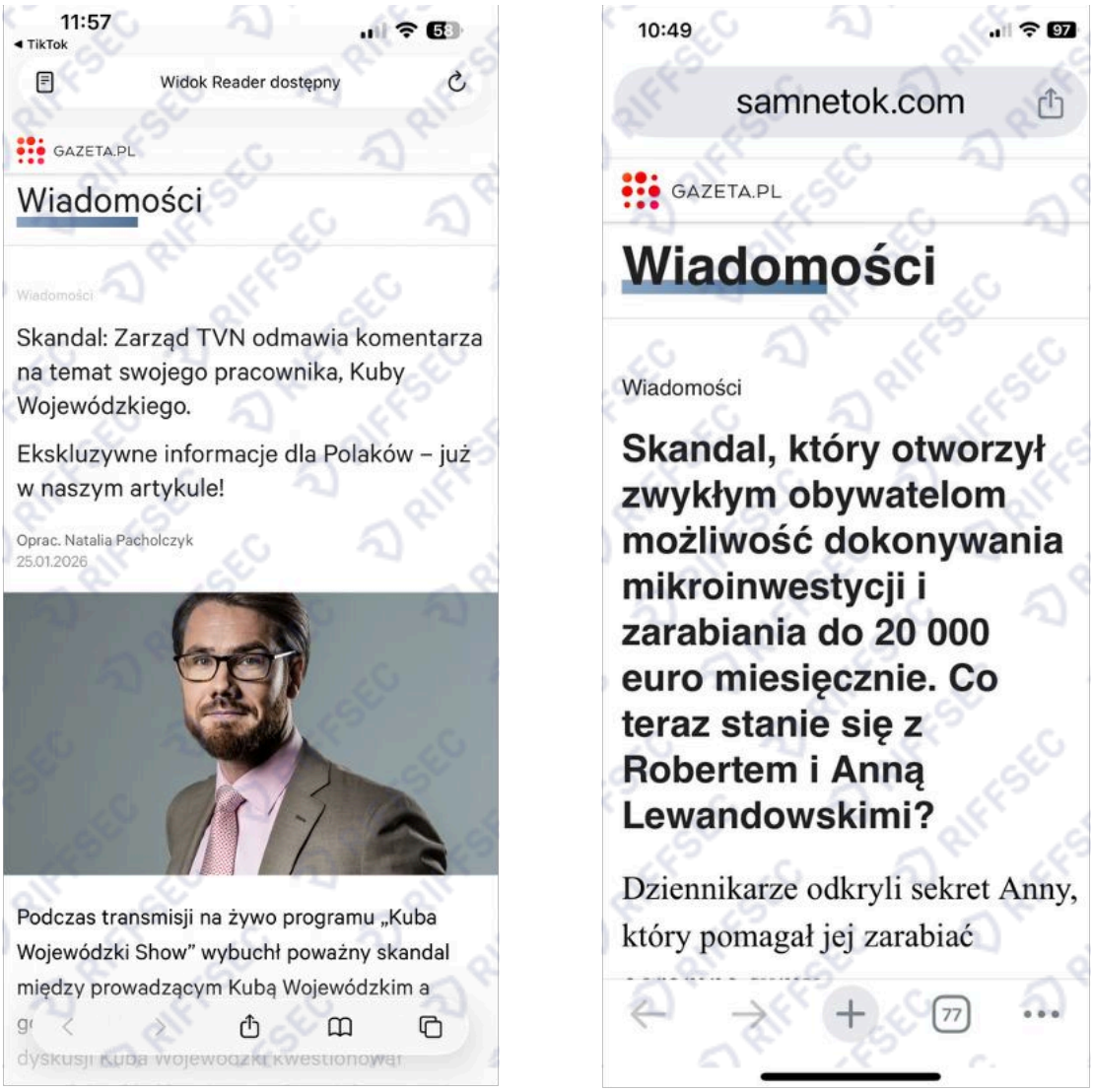
To kolejny kluczowych moment w tym schemacie działania przestępców. Po kliknięciu w reklamę użytkownik może zostać skierowany do jednego z dwóch rozwiązań.

W pierwszym przypadku formularz kontaktowy pojawia się bezpośrednio w obrębie portalu lub platformy, na której wyświetlana była reklama. W drugim przypadku użytkownik zostaje przekierowany na stronę internetową podszywające się pod istniejące portale informacyjne. W przeciwieństwie do wcześniejszych przykładów nie są to jednak legalne domeny. Na stronach tych publikowane są artykuły stylizowane na materiały prasowe, których celem (podobnie jak w przypadku reklam) jest wzbudzenie emocji u odbiorcy, na przykład poprzez sugestię skandalu lub sensacyjnego wydarzenia.



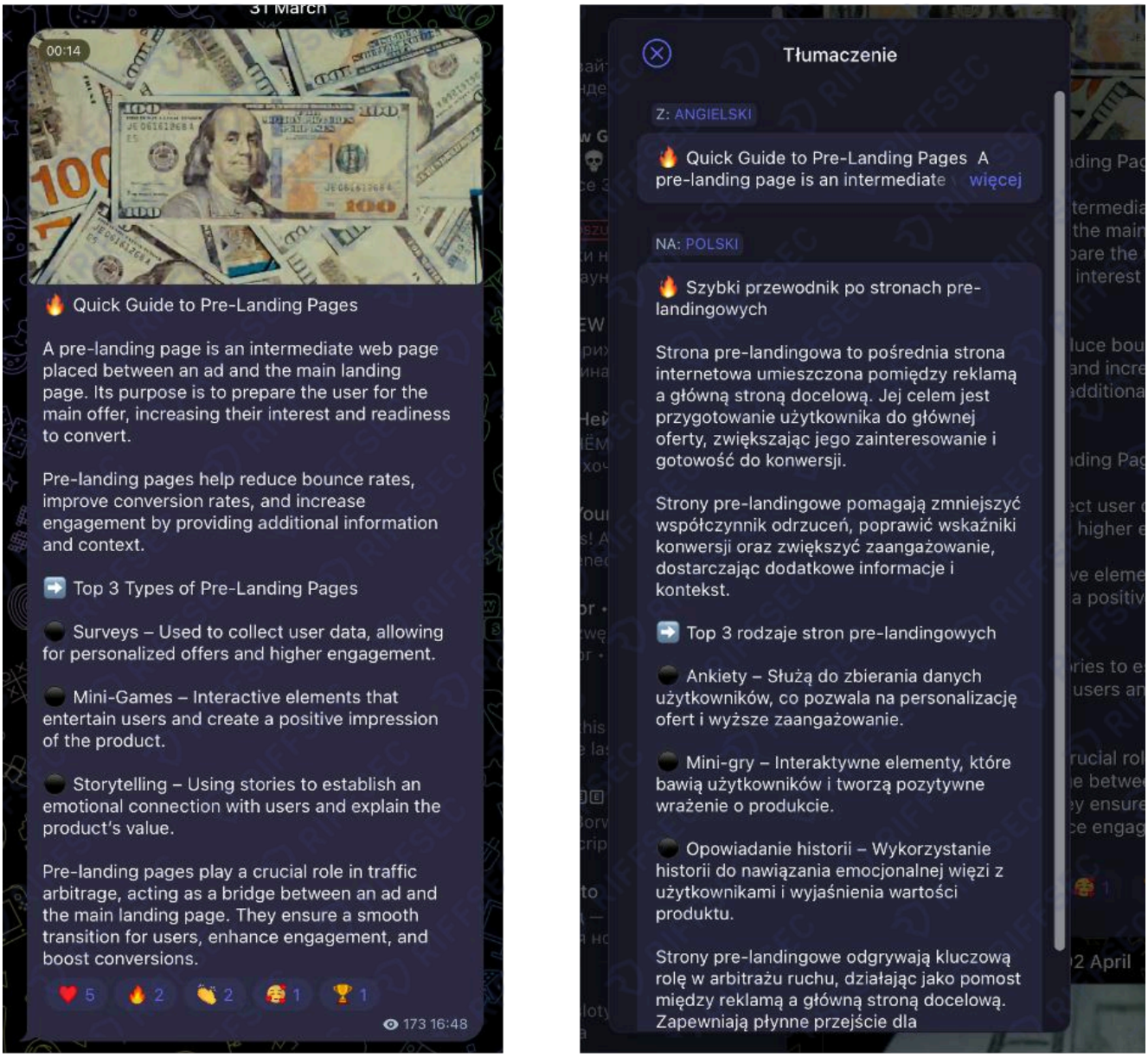
Widok reklamy z telefonu

Tego typu strony to kolejny element stosowanej przez przestępców gry socjotechnicznej. Nazywają je stronami pre-landingowymi.



Strona pre-lendingowa

Jak wskazują sami przestępcy, strony pre-landingowe stanowią pośredni etap pomiędzy reklamą, a formularzem do wypełnienia. Ich zadaniem jest przygotowanie użytkownika do głównej oferty poprzez zwiększenie jego zainteresowania oraz gotowości do podjęcia dalszego działania. Poniżej przedstawiono zrzut ekranu (wraz z tłumaczeniem) z jednej z grup przestępczych, w której omawiany jest sposób wykorzystywania tego typu stron.



Opinia przestepców nt. stosowania stron pre-lendingowych + tłumaczenie

Na tego typu stronach przestępcy starają się także udowodnić, że proces „zarabiania" brzmiący skomplikowanie jest prosty i łatwy do wykonania. W tym celu często prezentują instrukcje pokazujące krok po kroku, jakie działania należy podjąć. Ma to na celu zwiększenie zaufania osoby, którą chcą oszukać i wywołać złudzenie profesjonalizmu. Przykładową publikację „szybkich kroków ku bogactwu" przedstawiają kolejne grafiki.

Przykładowa strona pre-lendingowa

KROK 3:

"Poczekaj na telefon od menedżera Orlen, który zadzwoni do Ciebie w ciągu 24 godzin. Nie przegap tej rozmowy, bo nie będziesz mógł ponownie aplikować. Inna osoba zajmie Twoje miejsce".

UWAGA! MENEDŻER MOŻE ZADZWONIĆ Z NUMERU MIĘDZYNARODOWEGO, POŁĄCZENIE JEST BEZPŁATNE.

KROK 4:

"Następnie zostaniesz poproszony o dokonanie wpłaty w wysokości 1000 zł, aby program mógł rozpocząć handel. Zacznij od tej minimalnej kwoty. W ten sposób bezpiecznie upewnisz się, że platforma działa skutecznie. Nie martw się, te pieniądze pozostaną na Twoim koncie, depozyt jest potrzebny, aby system mógł zacząć kupować i sprzedawać aktywa, jak powiedziałem wcześniej.

Menedżer odpowie również na wszystkie pytania, pomoże w rejestracji i zrozumieniu programu."

Przykładowa strona pre-lendingowa

KROK 5:

"Po wykonaniu poprzednich kroków zostaniesz partnerem programu Orlen i zaczniesz zarabiać na sprzedaży aktywów! Wszystko, co musisz zrobić, to obserwować, wypłacać i wydawać swoje pieniądze."

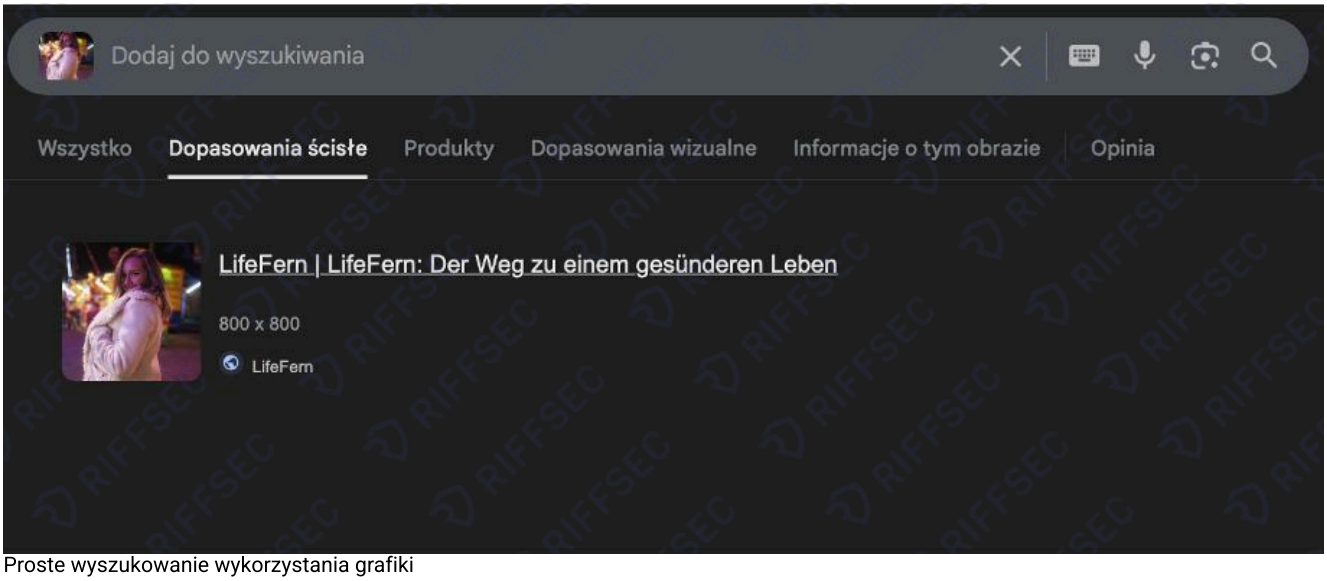
Dorota Gawryluk: "To jest po prostu niesamowite!"

Przykładowa strona pre-lendingowa

Na jednym z forów przestępczych pojawiła się informacja, że strona jest postrzegana jako bardziej wiarygodna, gdy przedstawia rzekomych pracowników firmy. W konsekwencji przestępcy zaczęli stosować ten element również na tworzonych przez siebie stronach.

Wizerunek rzekomych pracowników

Jednocześnie to samo zdjęcie (często generowane przy użyciu narzędzi sztucznej inteligencji, lub po prostu skradzione publicznie udostępnionych zdjęć w internecie) jest wykorzystywane na wielu różnych stronach. W efekcie możliwe jest jego łatwe zidentyfikowanie poprzez proste wyszukiwanie obrazu w Google Grafika, a tym samym odkrycie innych „kreacji" fałszywych stron.



Proste wyszukowanie wykorzystania grafiki

Zdjęcie tej samej osoby na róznych stron, pod róznymi nazwiskami

Na stronach pojawiają się również komentarze przygotowane przez przestępców. Przygotowane w różnych językach, w zależności do tej do jakiej grupy kierowana jest konkretna strona phishingowa. To kolejny element zwiększania wiarygodności publikowanych treści oraz zachęcenia użytkownika do skorzystania z prezentowanej oferty, oraz dowód na to że kampanie fałszywych inwestycji nie ograniczają się do konkretnego, jednego kraju i mają zasięg międzynarodowy.

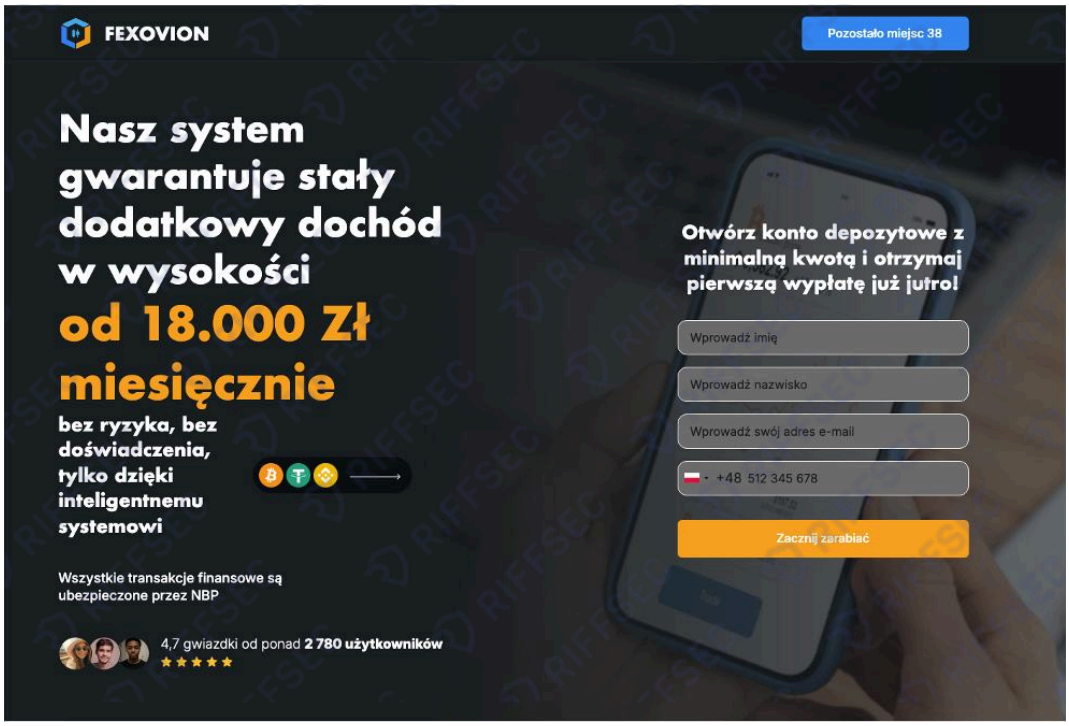
```
<script>
    let language = '<?= $language; ?>';

    const translations = {
        en: {
            title: "Congratulations on your successful registration in the system.",
            text: "You will receive a call within 24 hours - don't miss it, otherwise you might be interesting for another subscriber!"
        },
        de: {
            title: "Herzlichen Glückwunsch zur erfolgreichen Registrierung im System.",
            text: "Sie erhalten innerhalb von 24 Stunden einen Anruf - verpassen Sie ihn nicht, sonst könnte es für einen anderen Abonnenten interessant
        },
        ru: {
            title: "Поздравляем с успешной регистрацией в системе.",
            text: "Вы получите звонок в течение 24 часов - не пропустите его, иначе вы можете заинтересовать другого абонента!"
        },
        it: {
            title: "Congratulazioni per la tua registrazione avvenuta con successo nel sistema.",
            text: "Riceverai una chiamata entro 24 ore - non perderla, altrimenti potresti essere interessante per un altro abbonato!"
        },
        tr: {
            title: "Sisteme başarılı kaydınızdan dolayı tebrikler.",
            text: "24 saat içinde bir arama alacaksınız - kaçırmayın, aksi takdirde başka bir abone için ilginç olabilirsiniz!"
        },
        pt: {
            title: "Enhorabuena por su registro.",
            text: "En un plazo de 24 horas recibirá una llamada: ¡no la pierda, de lo contrario puede interesar a otro abonado!"
        },
        pl: {
            title: "Gratulacje z okazji pomyślnej rejestracji w systemie.",
            text: "Otrzymasz telefon w ciągu 24 godzin - nie przegap go, w przeciwnym razie możesz być interesujący dla innego abonenta!"
```
Przygotowane szablony komentarzy

```
},
hu: {
    title: "Gratulálok a sikeres regisztrációhoz a rendszerben.",
    text: "24 órán belül fog kapni egy hívást – ne hagyja ki, különben egy másik előfizető számára is érdekes lehet!"
},
ro: {
    title: "Felicitări pentru înregistrarea dvs. reușită în sistem.",
    text: "Veți primi un apel în termen de 24 de ore – nu-l ratați, altfel puteți fi interesant pentru un alt abonat!"
},
ae: {
    title: "تهانينا على تسجيلك الناجح في النظام.",
    text: "ستتلقى مكالمة في غضون 24 ساعة – لا تفوتها، وإلا فقد تكون مثيرة للاهتمام بالنسبة لمشترك آخر!"
},
jp: {
    title: "システムへのご成功登録おめでとうございます。",
    text: "24時間以内にお電話を差し上げますので、お見逃しなく。それ以外の場合、他の加入者にとって興味深いかもしれません！"
},
br: {
    title: "Parabéns pelo seu registro bem-sucedido no sistema.",
    text: "Você receberá uma ligação dentro de 24 horas – não perca, caso contrário, você pode ser interessante para outro assinante!"
},
ca: {
    title: "Congratulations on your successful registration in the system.",
    text: "You will receive a call within 24 hours – don't miss it, otherwise you might be interesting for another subscriber!"
},
sg: {
    title: "Sistemde başarılı kaydınız için tebrikler.",
    text: "24 saat içinde bir çağrı alacaksınız – kaçırmayın, aksi takdirde başka bir abone için ilginç olabilirsiniz!"
},
hk: {
    title: "系統中的成功註冊，恭喜.",
    text: "您將在24小時內收到一通電話 – 請勿錯過，否則您可能對其他訂閱者有興趣！"
},
```

Przygotowane szablony komentarzy

Po przejściu przez opisane wcześniej etapy użytkownik trafia do docelowego elementu całego schematu, czyli formularza kontaktowego. Formularz ten służy do pozyskania podstawowych danych, takich jak imię, nazwisko (nie zawsze), adres e-mail oraz numer telefonu. Na tego typu stronach nie są wymagane żadne dodatkowe informacje. Zebranie tych podstawowych danych jest wystarczające, aby przestępcy mogli przejść do kolejnego etapu działania, a jednocześnie nie wzbudza podejrzenia ofiary, bo przecież nie musi podawać haseł czy danych płatniczych (co mogło by wzbudzić podejrzenia, lub zniechęcić ofiarę do dalszej interakcji). Przykładowe formularze poniżej:

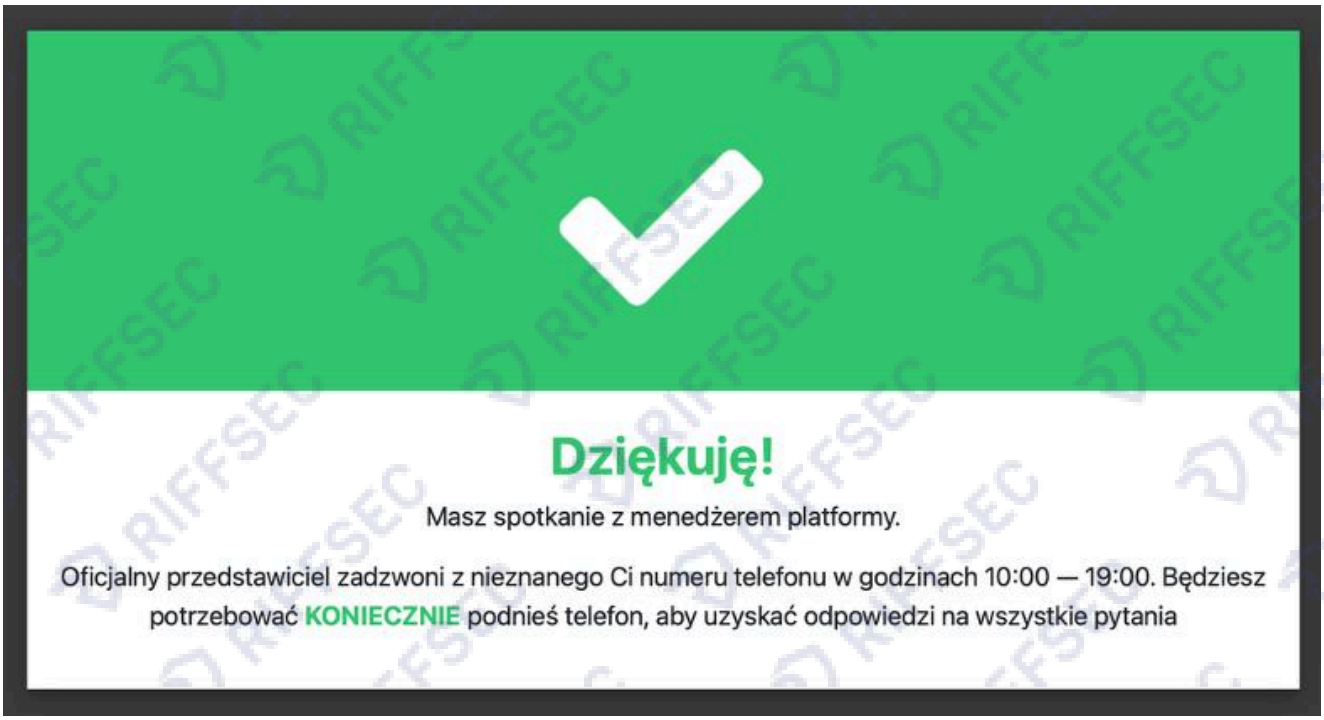


Przykładowe kreacje formularzy

Przykładowe kreacje formularzy

> Ograniczony zakres wymaganych danych na tym etapie sprzyja powstawaniu błędnego przekonania, że ich przekazanie nie wiąże się z istotnym ryzykiem. Użytkownicy często traktują podanie podstawowych informacji, takich jak imię, numer telefonu czy adres e-mail, jako działanie neutralne. rzeczywistości to istotny punkt wejścia do dalszej manipulacji i może prowadzić do poważnych strat finansowych.

Po wypełnieniu formularza na stronie zazwyczaj pojawia się komunikat informujący, że z użytkownikiem skontaktuje się doradca inwestycyjny, menedżer platformy lub inny przedstawiciel. Nazwy stanowisk używane w komunikacie mogą się różnić, gdyż nazewnictwo zależy od przyjętej przez daną grupę przestępczą narracji. W rzeczywistości jest to kolejny element scenariusza przygotowanego przez przestępców, sugerujący „legalność" oferty.



Komunikat przygotowany przez atakujących

Co dzieje się w momencie, gdy dochodzi do rozmowy telefonicznej? To właśnie wtedy rozpoczyna się kolejny kluczowy etap manipulacji prowadzonej przez przestępców.

Etap trzeci: telefon od przestępcy

Kolejnym kluczowym momentem w tym schemacie oszustwa jest bezpośredni kontakt przestępców z ofiarą. Z perspektywy osoby poszkodowanej obecnie jest w sytuacji, w której:

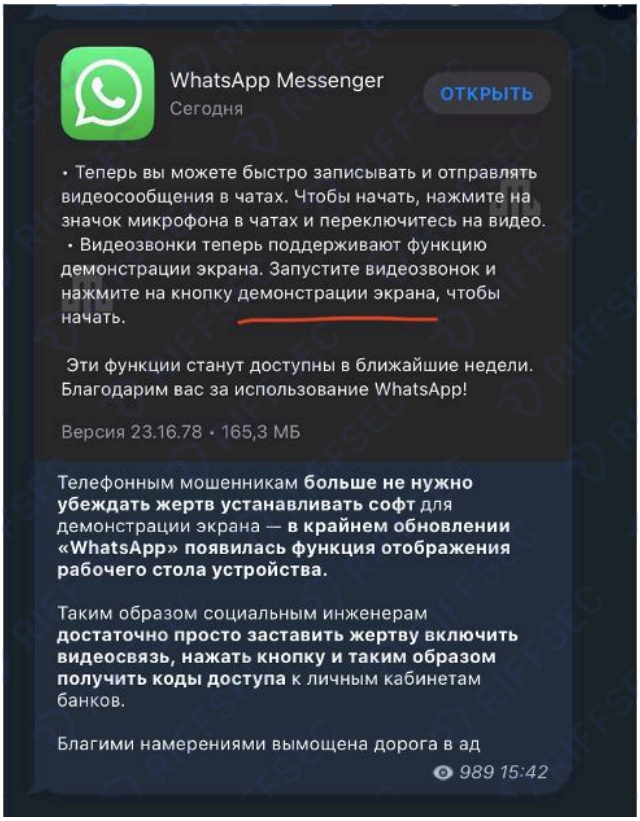
1. zobaczył/a reklamę, zainteresował/a się nią, zapoznał/a się z treścią i kliknęła w link,
2. [opcjonalnie] trafił/a na stronę, na której przeczytał/a artykuł dotyczący rzekomych inwestycji oraz historii osób, które miały dzięki nim osiągnąć wysokie zyski,
3. wypełnił/a formularz kontaktowy i oczekuje na dalszy kontakt, który zazwyczaj następuje w bardzo krótkim czasie.

Szybki kontakt ze strony przestępców jest możliwy dzięki wykorzystywanym przez nich narzędziom, o których będzie mowa w dalszej części raportu. Szybka reakcja przestępców ma znaczenie psychologiczne, przestępcy wiedzą, że trafiają na osobę, która przed chwilą wyraziła zainteresowanie ofertą, jest jej ciekawa i nie miała jeszcze kiedy przemyśleć sytuacji czy porozmawiać z kimś trzecim lub zweryfikować „ofertę".

Rozmowa telefoniczna stanowi kolejny etap manipulacji. Na początku pojawiają się gratulacje oraz wizja szybkiego osiągnięcia zysku w krótkim czasie. Następnie ofiara otrzymuje informację o rzekomym przyznaniu dostępu do „platformy inwestycyjnej" (nazewnictwo może się różnić w zależności od przyjętego scenariusza). Jednocześnie przestępcy proszą o zainstalowanie programu „pomagającego", który w rzeczywistości jest narzędziem zdalnego dostępu do urządzenia (telefon, komputer). dostępu do urządzenia (telefon, komputer). Celem takiego działania jest uzyskanie możliwości obserwowania czynności wykonywanych przez ofiarę na jej urządzeniu lub też bezpośrednia na nim interakcja. W tym celu przestępcy często wykorzystują legalne narzędzia w sposób niezgodny z ich przeznaczeniem, proponując instalację takich aplikacji jak TeamViewer, AnyDesk czy UltraViewer.

> Wykorzystanie legalnych narzędzi do celów oszukańczych staje się coraz częstszą praktyką, nie tylko w zakresie omawianego scenariusza fałszywych inwestycji. W marcu tego roku CISA oraz FBI wydały komunikat, zwracając uwagę na rosnącą skalę nadużyć legalnych narzędzi do zdalnego zarządzania (RMM - Remote Monitoring and Management) w atakach ransomware i nie tylko. Atakujący wykorzystują popularne, podpisane cyfrowo aplikacje administracyjne jako mechanizm trwałego dostępu do środowisk firmowych. Ze względu na ich legalny charakter, narzędzia te często nie są blokowane przez standardowe zabezpieczenia antywirusowe. Zdaje się, że to element niejednokrotnie niesłusznie pomijany w krajobrazie zagrożeń, a stanowi coraz istotniejszy wektor ataku w rękach atakujących.

Przestępcy zaczęli również wykorzystywać funkcje komunikatorów internetowych. Biorąc pod uwagę fakt, że atakujący z ofiarami najczęściej kontaktują są poprzez WhatsApp, to funkcja udostępniania ekranu jest dla nich bardzo użyteczna.
W takim scenariuszu wystarczy nakłonić ofiarę do rozpoczęcia połączenia wideo (zamiast standardowego połącznia) oraz włączenia udostępniania ekranu. To pozwala przestępcy obserwować działania wykonywane na urządzeniu i odpowiednio manipulować ofiarą.



Przestępcy opisują funkcje komunikatora wrac z tłumaczeniem

W wielu przypadkach osoby mniej zaawansowane technologicznie nie zdają sobie sprawy, że w ten sposób udostępniły widok swojego ekranu osobie trzeciej. Poniżej przedstawiono zrzut ekranu z jednej z grup przestępczych, w której przekazywano informacje o możliwości wykorzystania tej funkcji.

Tłumaczenie

Teraz możesz szybko nagrywać i wysyłać wiadomości wideo w czatach. Aby zacząć, naciśnij ikonę mikrofonu w czacie i przełącz się na wideo. Połączenia wideo obsługują teraz funkcję udostępniania ekranu. Uruchom połączenie wideo i naciśnij przycisk udostępniania ekranu, aby rozpocząć. Funkcje te będą dostępne w najbliższych tygodniach. Dziękujemy za korzystanie z WhatsApp!

Wersja 23.16.78, 165,3 MB

Dalej tekst pod obrazkiem: Telefoniczni oszuści nie muszą już przekonywać ofiar do instalowania oprogramowania do udostępniania ekranu.
W najnowszej aktualizacji WhatsApp pojawiła się funkcja wyświetlania ekranu urządzenia.

Innym powodem dlaczego kontakt z ofiarami najczęściej odbywa się za pośrednictwem komunikatora WhatsApp to kwestia korzystania z kart SIM. Nawet w sytuacji, gdy numer telefonu przestaje być aktywny lub dostęp do niego jest ograniczony, komunikator może nadal funkcjonować. Dzięki temu przestępcy mogą utrzymywać kontakt z ofiarą bez większych przeszkód, a jednocześnie nie musza ponosić kosztów i straty czasu na częste zmiany numerów telefonu.

W trakcie komunikacji atakujący stosują różne techniki manipulacyjne, dostosowując je do reakcji i zachowania potencjalnej ofiary. Przykłady:

- w odpowiedzi na informację, że dana osoba chce omówić temat inwestycji z małżonkiem, przestępca może próbować podważyć potrzebę konsultacji, sugerując, że jest to samodzielna decyzja finansowa, a partner w przyszłości będzie jedynie wdzięczny za podjęcie takiej inicjatywy,

- w sytuacji, gdy rozmówca deklaruje zainteresowanie inwestycją, ale jednocześnie waha się przed podjęciem decyzji, przestępca może poinformować o „przełączeniu" rozmowy do menedżera, kierownika lub dyrektora. W rzeczywistości rozmowę przejmuje inna osoba z tej samej grupy przestępczej, często bardziej doświadczona w prowadzeniu manipulacji. Sam motyw „przełączenia" ma wywołać u ofiary poczucie, że jej sprawa jest traktowana poważnie i wymaga wyższego poziomu obsługi,

- w przypadku pojawienia się wątpliwości, próśb o wypłatę środków lub frustracji związanej z ich brakiem, przestępcy często próbują zbudować pozorną relację z ofiarą. Może to polegać na zaproponowaniu przejścia na mniej formalny sposób komunikacji, opowiadaniu o rzekomej rodzinie, doświadczeniu zawodowym czy planach prywatnych.

Strategii stosowanych przez przestępców jest znacznie więcej. Ich głównym celem jest utrzymanie kontaktu z ofiarą oraz podtrzymanie jej zaangażowania w rzekomą inwestycję. Kontakt w takich przypadkach nie jest jednorazowy, przestępcy podszywając się pod doradców lub menedżerów inwestycyjnych, regularnie informują o rzekomym wzroście wartości środków zgromadzonych na platformie.

> Przestępcy sprawiają, że ofiara czuję się zaopiekowana. Dzwonią i piszą do niej na WhatsApp, przysyłają maile, informują o wzroście inwestycji, a czasem po prostu pytają jak się ma, co u niej słychać. Im bardziej czuję się „dobrze" w tej relacji, tym trudniej jest jej uwierzyć, że po drugiej stronie jest grupa przestępcza. Zmanipulowanej ofierze wydaje się, że poznała drugą stronę, że będąc zawsze miłym do niej, nie mógł przecież chcieć jej oszukać. Tymczasem rzeczywistość okazuje się przykra...

Jednocześnie zachęcają ofiarę do wykonywania kolejnych wpłat. W tym celu podawane są numery rachunków bankowych (zarówno krajowych, jak i zagranicznych) a także instrukcje dotyczące dokonywania przelewów w kryptowalutach. Zdarza się również, że ofiary są instruowane, aby wypłacić gotówkę i wpłacić ją fizycznie we wpłatomatach lub kryptomatach. Działania te mają na celu utrudnienie identyfikacji i śledzenia przepływu środków finansowych.

Zdarzają się także sytuacje, w których jednej ofierze podawany jest rachunek bankowy należący do innej osoby pokrzywdzonej. W ten sposób od jednej osoby wyłudzane są środki, podczas gdy druga otrzymuje przelew, który ma sprawiać wrażenie zwrotu z inwestycji. W środowiskach przestępczych funkcjonuje przekonanie, że nawet niewielka wypłata może zwiększyć zaufanie ofiary i skłonić ją do wykonania kolejnych przelewów, często wielokrotnie przewyższających wartość otrzymanego zwrotu.

I niestety to przekonanie jest bardzo słuszne. Wejdźmy w buty ofiary, która jest już na etapie wpłacania kolejnych środków, silnie zmanipulowana. Wokół niej zaczynają pojawiać się ludzie, którzy (delikatnie mówiąc) poddają w wątpliwości rzekomą inwestycję. I co ona słyszy? A np. to, że nigdy żadnych pieniędzy nie dostanie. Zaczyna sama mieć wątpliwości, chce się upewnić i wtedy dostaje przelew. Nawet jeżeli jest on stosunkowo niewielki, do tego co już wpłaciła, to mechanizm jest niezwykle prosty. Skoro dostała przelew, to oznacza, że wszyscy, którzy ją ostrzegali jednak się mylili, a decyzja o inwestowaniu była słuszna. Mało tego, przestępca w rozmowach będzie podsycać to przekonanie mówiąc, że ludzie zazdroszczą, banki nie chcą żeby ludzie obracali pieniędzmi poza „ich systemem finansowym" (czymkolwiek jest), a policja jest skorumpowana. Efekt? Pogłębienie manipulacji, zwiększenie zaufania ofiary do przestępcy, a w konsekwencji oddanie tego przelewu i zrobienie kolejnych na rzecz atakujących.

Agnieszka Gryszczyńska

Doktor habilitowany nauk prawnych, inżynier informatyk, profesor uczelni w Katedrze Prawa Informatycznego na Wydziale Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie

Operowanie przy niskich kwotach na rachunkach pokrzywdzonych – pozwala również sprawcom nie dekonspirować rachunków służących do przyjmowania i prania większych kwot pieniężnych. Istotnie utrudnia również identyfikację rachunków tzw. słupów. Na tym etapie ofiara przez cały czas ma również dostęp do tzw. platformy inwestycyjnej. W rzeczywistości jest to strona przygotowana przez przestępców, która ma jedynie symulować działanie prawdziwego systemu inwestycyjnego. Prezentowane na niej „rosnące zyski" są jedynie symulacją kontrolowaną przez atakujących.

Przestępcza platforma inwestycyjna

Przestępcy wykorzystują również elementy, które mają sprawiać wrażenie profesjonalizmu i bezpieczeństwa platformy. W wielu przypadkach logowanie do rzekomej platformy inwestycyjnej odbywa się z wykorzystaniem mechanizmu dwuskładnikowego uwierzytelniania (2FA). Najczęściej jest to kod przesyłany na adres e-mail użytkownika. Oznacza to, że przestępcy przygotowali własne rozwiązanie technologiczne imitujące mechanizmy bezpieczeństwa stosowane w legalnych systemach. Celem takiego działania jest wzmocnienie poczucia wiarygodności platformy i jej bezpieczeństwa. Przestępcy wykorzystują fakt, że w przestrzeni publicznej często podkreśla się znaczenie stosowania dwuskładnikowego uwierzytelniania. Dzięki temu mogą przekonywać ofiary, że platforma jest bezpieczna, ponieważ „nawet kod zabezpieczający przychodzi na e-mail".

W ten sposób manipulacja może trwać przez wiele tygodni, a nawet miesięcy. W trakcie rozmów przestępcy przygotowują ofiarę również na ewentualne ostrzeżenia ze strony otoczenia lub instytucji finansowych. Mogą sugerować, że osoby trzecie będą próbowały zniechęcić ją do inwestowania z powodu zazdrości, a bank może zgłaszać wątpliwości, ponieważ niechętnie patrzy na przepływ środków poza tradycyjnym systemem finansowym.

W tym czasie środki finansowe stopniowo trafiają do przestępców. Sytuacja zmienia się zazwyczaj w momencie, gdy ofiara próbuje wypłacić zgromadzone na platformie „zyski". Zdarzają się przypadki, w których przestępcy dokonują niewielkiego przelewu, aby wzmocnić zaufanie ofiary (opisywaliśmy wcześniej). Jeżeli jednak osoba poszkodowana zaczyna domagać się większej wypłaty lub przestępcy zorientują się, że podejrzewa ona oszustwo, kontakt zostaje nagle przerwany. W takiej sytuacji pozostaje osoba poszkodowana, często bez oszczędności, niekiedy również z zaciągniętymi zobowiązaniami finansowymi. W wielu przypadkach pojawia się również silne poczucie wstydu, gdy ofiara zaczyna dostrzegać niespójności w całym schemacie działania przestępców. Można by przypuszczać, że na tym etapie historia się kończy. W rzeczywistości jednak w wielu przypadkach pojawia się jeszcze jeden etap działania przestępców.

Agnieszka Gryszczyńska

Doktor habilitowany nauk prawnych, inżynier informatyk, profesor uczelni w Katedrze Prawa Informatycznego na Wydziale Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie

Pokrzywdzony zazwyczaj na tym etapie składa zawiadomienie o podejrzeniu popełnienia przestępstwa. Istotne jest aby przekazał jak najwięcej informacji mogących prowadzić do ustalenia rachunków bankowych na które trafiły jego środki lub założonych na polecenie sprawców kont na giełdach kryptowalut. Kwalifikacja prawna przestępstwa będzie zależała od modus operandi sprawców. Jeśli zmanipulowany pokrzywdzony dokonywał wpłat na rachunek wskazany przez sprawców mamy do czynienia z przestępstwem oszustwa (tj. czynem z art. 286 k.k.). Jeśli pokrzywdzony zainstalował oprogramowanie do zdalnego pulpitu i sprawcy sami dokonywali transferów środków z rachunku pokrzywdzonego – podstawową kwalifikacją będzie przestępstwo hackingu (art. 267 k.k.) oraz kradzieży z włamaniem (art. 279 k.k.). Dodatkowo sprawcy ponoszą również odpowiedzialność za pranie pieniędzy (art. 299 k.k.). Istotnym utrudnieniem w pociągnięciu sprawców do odpowiedzialności karnej jest jednak transgraniczność tego typu czynów i konieczność korzystania z instrumentów międzynarodowej współpracy w sprawach karnych.

Etap dodatkowy: oszukać oszukanego

Na tym etapie sytuacja dla osób poszkodowanych często staje się jeszcze trudniejsza. Przestępcy dysponują bazą danych osób, które wcześniej padły ofiarą opisanego schematu. Wiedzą zatem, że są to osoby znajdujące się w trudnej sytuacji emocjonalnej i często finansowej oraz poszukujące możliwości odzyskania utraconych środków. W takich przypadkach osoby te mogą trafić na materiały informujące o rzekomej możliwości odzyskania utraconych pieniędzy (w formie połączenia telefonicznego lub reklamy w mediach społecznościowych). Co dzieje się dalej? Schemat działania pozostaje taki sam. Użytkownik trafia na formularz umożliwiający pozostawienie danych kontaktowych lub na stronę pre-landingową przygotowaną przez przestępców.

Reklamy typu „oszukać oszukanego”

Strona pre-lendingowa w dodatkowym etapie scenariusza przestępczego

Następnie scenariusz działania ponownie przebiega w podobny sposób. Z osobą poszkodowaną kontaktuje się przestępca, informując ją o możliwości odzyskania utraconych środków. Warunkiem ma być jednak dokonanie określonej opłaty. W ten sposób osoba, która została już wcześniej oszukana, może ponownie stracić pieniądze. Mechanizm ten polega na wykorzystaniu emocji oraz nadziei związanej z możliwością odzyskania utraconych środków.

Alternatywnie formularz może być osadzony bezpośrednio w mediach społecznościowych.

Formularz kontaktowy

Również na tym etapie przestępcy stosują różne techniki manipulacyjne, w tym podszywanie się pod znane marki, instytucje lub osoby publiczne, a także materiały wideo typu deepfake. Co istotne, wiele takich nagrań rozpoczyna się od komunikatów ostrzegających przed oszustwami finansowymi. Przestępcy często wykorzystują w nich sformułowania bardzo zbliżone do tych, które pojawiają się w oficjalnych komunikatach edukacyjnych.

Analiza CTI, czyli świat przestępczy

Jak wynika z przedstawionego scenariusza, schemat ten jest na tyle złożony i wieloetapowy, że jego realizacja nie może być przypisywana pojedynczej osobie działającej samodzielnie. W praktyce mamy do czynienia ze zorganizowanymi strukturami przestępczymi, które funkcjonują w sposób przypominający działalność przedsiębiorstw. W ramach takich struktur można zaobserwować wyraźny podział ról. W szczególności wyróżnić można tzw.:

- korporacje leadowe, odpowiedzialne za pozyskiwanie danych kontaktowych potencjalnych ofiar,
- korporacje telefoniczne (call center), których zadaniem jest bezpośredni kontakt z ofiarami oraz prowadzenie dalszej manipulacji.

Coraz częściej wskazuje się również na rozwój modelu określanego jako Crime-as-a-Service (CaaS), w ramach którego poszczególne elementy infrastruktury atakujących są oferowane od innych grup przestępczych w formie usług.

Korporacje lead'owe

Ta gałąź przestępczego rynku jest młodsza niż działalność przestępczych call center, co nie oznacza jednak, że jest obecnie mniej rozwinięta. Mowa o etapie odpowiedzialny za dystrybucję reklam w Internecie oraz pozyskiwanie danych kontaktowych potencjalnych ofiar.

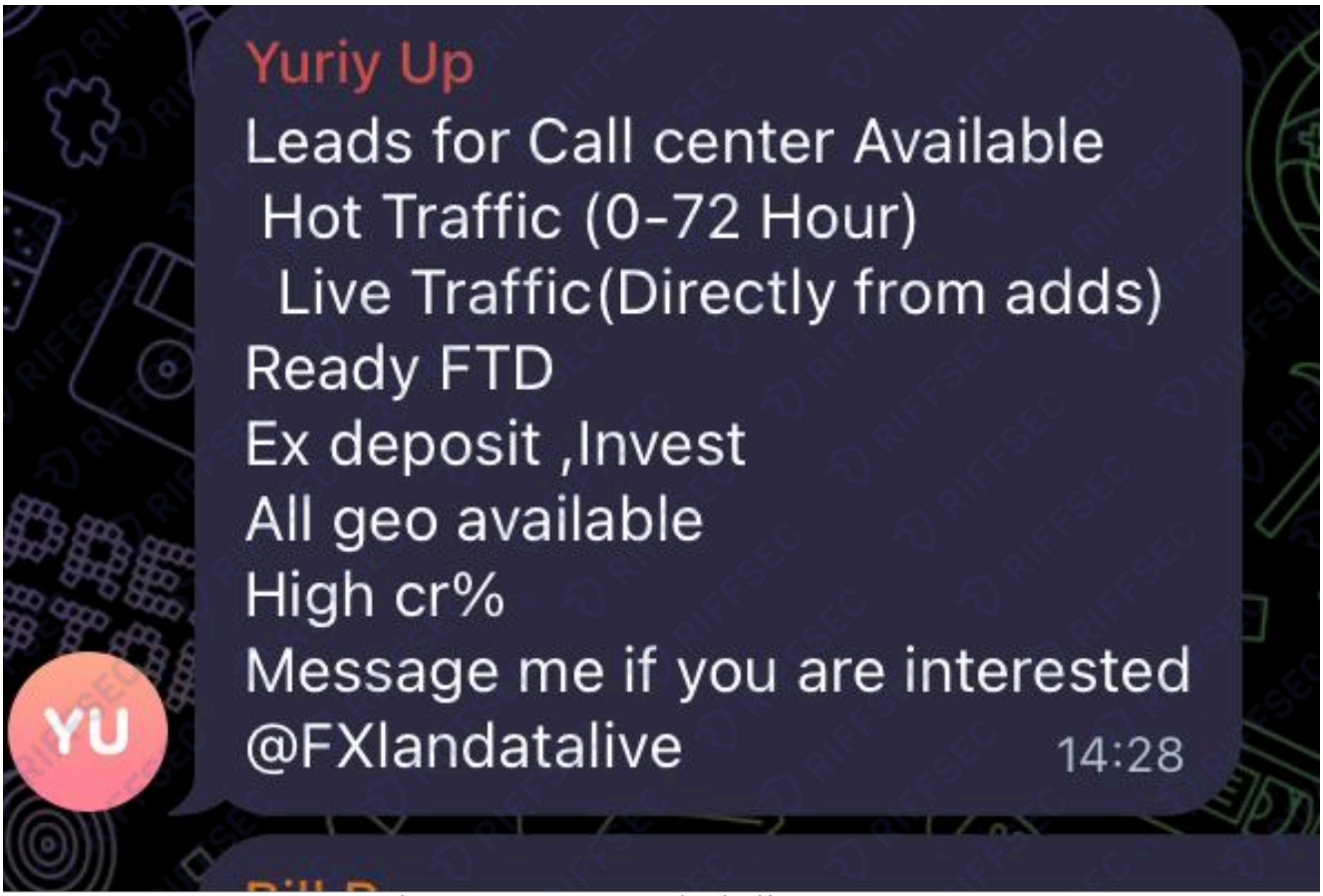
Przez długi czas działania te były prowadzone przez pojedyncze osoby funkcjonujące w modelu afiliacyjnym. Mechanizm ten jest dobrze znany również w legalnym marketingu internetowym. Polegał on na przygotowaniu reklamy, umieszczeniu jej w programie afiliacyjnym, a następnie na dystrybucji materiałów przez osoby korzystające z indywidualnych linków, które publikowały je w mediach społecznościowych.

> Osoby uczestniczące w programach afiliacyjnych często nie miały świadomości charakteru rozpowszechnianych treści. Otrzymywały gotowe kreacje reklamowe, nie znając języka ich publikacji ani osób, których wizerunek był wykorzystywany, nie dostrzegały (lub nie chciały dostrzegać) niczego niepokojącego. Kluczowym wskaźnikiem pozostawała dla nich liczba kliknięć, bo to przekładało się na ich zarobki. To wszystko sprzyjało dalszej dystrybucji materiałów wykorzystywanych w oszustwie.

Z czasem przestępcy dostrzegli jednak, że jest to istotny element całego procesu, który można lepiej zorganizować i wykorzystać na większą skalę, a tym samym pozyskać więcej korzyści majątkowych. W rezultacie zaczęły powstawać wyspecjalizowane grupy zajmujące się pozyskiwaniem tzw. leadów.

Lead oznacza zestaw podstawowych danych pozostawionych przez użytkownika w formularzu kontaktowym, takich jak imię, nazwisko (nie zawsze wymagane), adres e-mail oraz numer telefonu. Do tych informacji często dołączane są dodatkowe dane, na przykład informacja o tym, która reklama doprowadziła do pozostawienia danych, jaki wizerunek został w niej wykorzystany, a także czas kliknięcia reklamy i wypełnienia formularza.
Tak przygotowane zestawy danych, obejmujące od kilku do kilkudziesięciu, a w niektórych przypadkach nawet kilkaset kontaktów, są następnie wystawiane na sprzedaż w środowiskach przestępczych.Rozwój tego rynku sprawił, że coraz więcej grup przestępczych zaczęło specjalizować się właśnie w pozyskiwaniu i sprzedaży leadów. Rosnąca liczba podmiotów działających w tym obszarze doprowadziła również do powstania konkurencji na przestępczym rynku, co z kolei wpłynęło na rozwój ofert oraz sposobów sprzedaży takich danych. W kolejnej części raportu przedstawiono przykłady ofert publikowanych przez przestępców, ilustrujących sposób sprzedaży tego typu leadów.

W ogłoszeniach przestępcy m.in deklarują, że dysponują leadami pochodzącymi z różnych lokalizacji geograficznych. Często kraj z którego pochodzą leady, decyduje o cenie. Podkreślają również, że są to dane „świeże” oraz tzw. live traffic, czyli kontakty pozyskane i udostępnione bezpośrednio z aktywnych kampanii reklamowych.

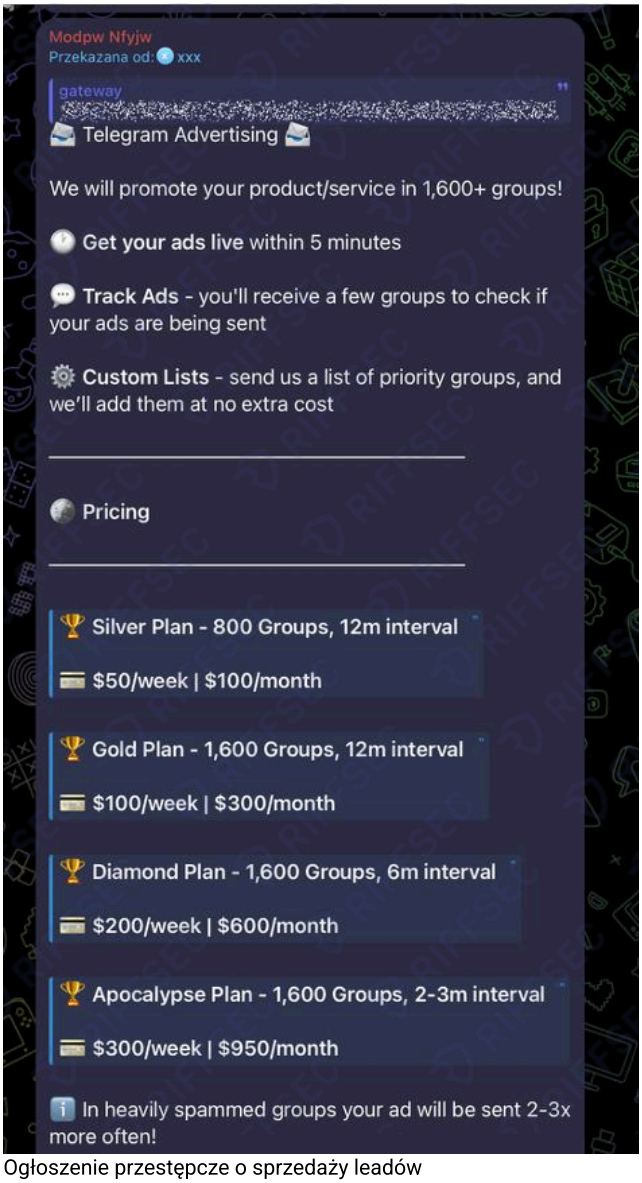


Ogłoszenie przestępcze o sprzedaży leadów

W ofertach pojawia się również możliwość uzyskania dostępu do platform typu CRM. Po wykupieniu dostępu użytkownik (w tym przypadku inny przestępca) otrzymuje możliwość bieżącego podglądu napływających danych potencjalnych ofiar, które zainteresowały się określoną kampanią reklamową, konkretnym wzorem reklamy lub ruchem pochodzącym z danej platformy.Dostęp do takich danych jest utrzymywany tak długo, jak długo opłacana jest usługa.

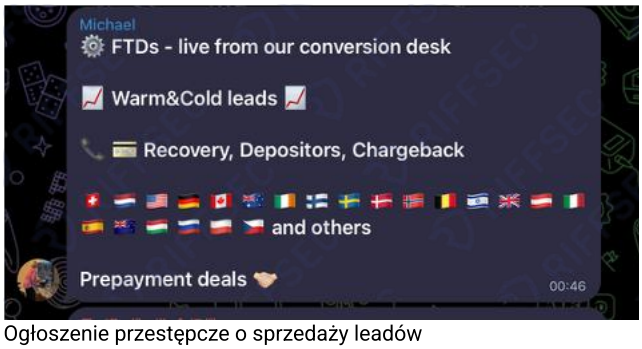
W praktyce oznacza to, że w momencie gdy potencjalna ofiara zobaczy reklamę np. na Facebooku, zainteresuje się nią, przejdzie na stronę i pozostawi swoje dane w formularzu, informacja ta może trafić do systemu w czasie rzeczywistym. W efekcie już po kilku minutach od wypełnienia formularza użytkownik może otrzymać połączenie telefoniczne od osoby podszywającej się pod doradcę inwestycyjnego. W rzeczywistości będzie to przestępca działający w strukturze przestępczego call center, które wykupiło dostęp do takich danych od korporacji leadowych.

Dostęp do leadów wykupuje się w modelu subskrypcyjnym. Kupujący (przestępca) płaci za to czego potrzebuję lub na co go stać.



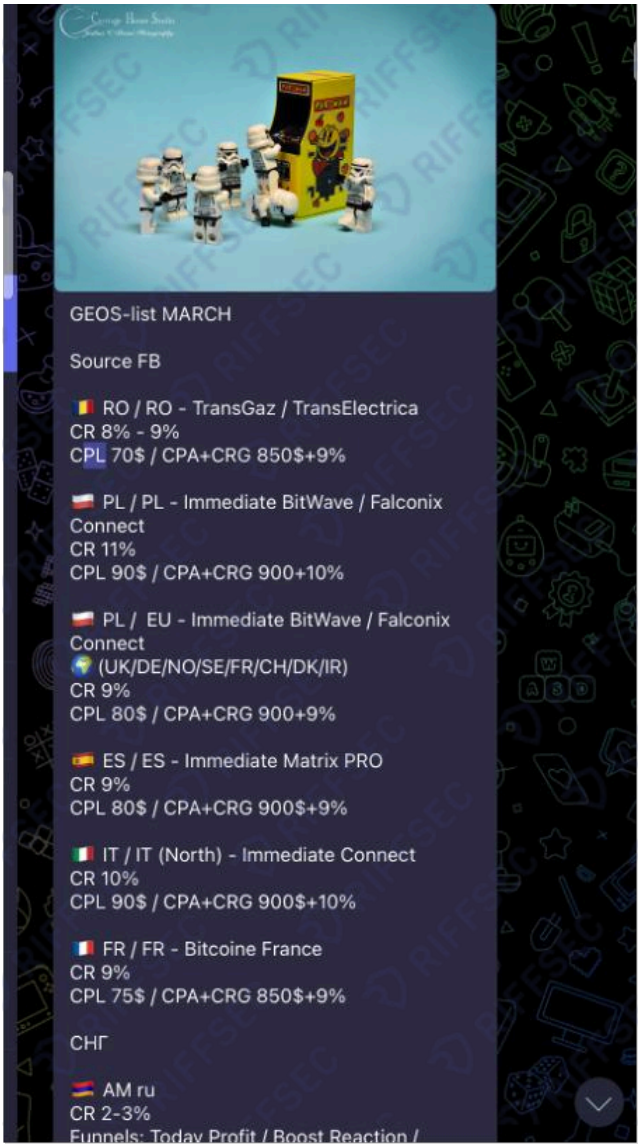
Ogłoszenie przestępcze o sprzedaży leadów

Ogłoszenie przestępcze o sprzedaży leadów



Ogłoszenie przestępcze o sprzedaży leadów

W ofertach sprzedaży leadów przestępcy często wskazują również źródło ruchu, czyli miejsce, w którym potencjalna ofiara zobaczyła reklamę. Może to być na przykład Facebook lub inne platformy reklamowe. Informacja ta pozwala kupującym lepiej zrozumieć kontekst pozyskania danych oraz dopasować sposób prowadzenia rozmowy z potencjalną ofiarą.

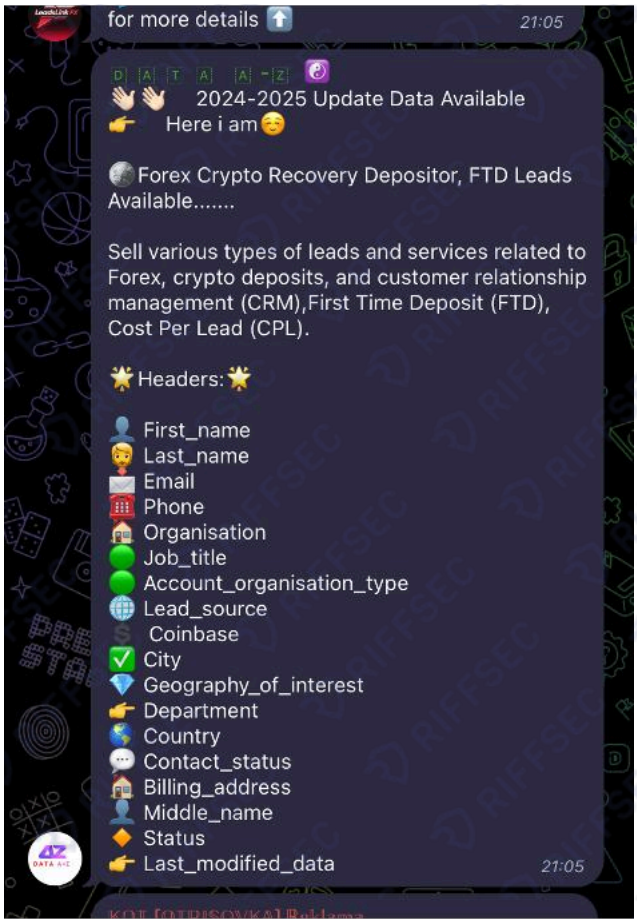


Ogłoszenie przestępcze o sprzedaży leadów

W niektórych ofertach przestępcy deklarują również możliwość złożenia reklamacji dotyczącej jakości otrzymanych leadów. W takich przypadkach oferują wymianę danych kontaktowych lub przekazanie nowych leadów w sytuacji, gdy przekazane informacje okażą się nieaktualne lub nieprawidłowe.

W ofertach podkreślana jest również dostępność wsparcia technicznego lub operacyjnego. Sprzedający deklarują możliwość kontaktu w przypadku problemów z otrzymanymi leadami lub innymi elementami oferowanej usługi.

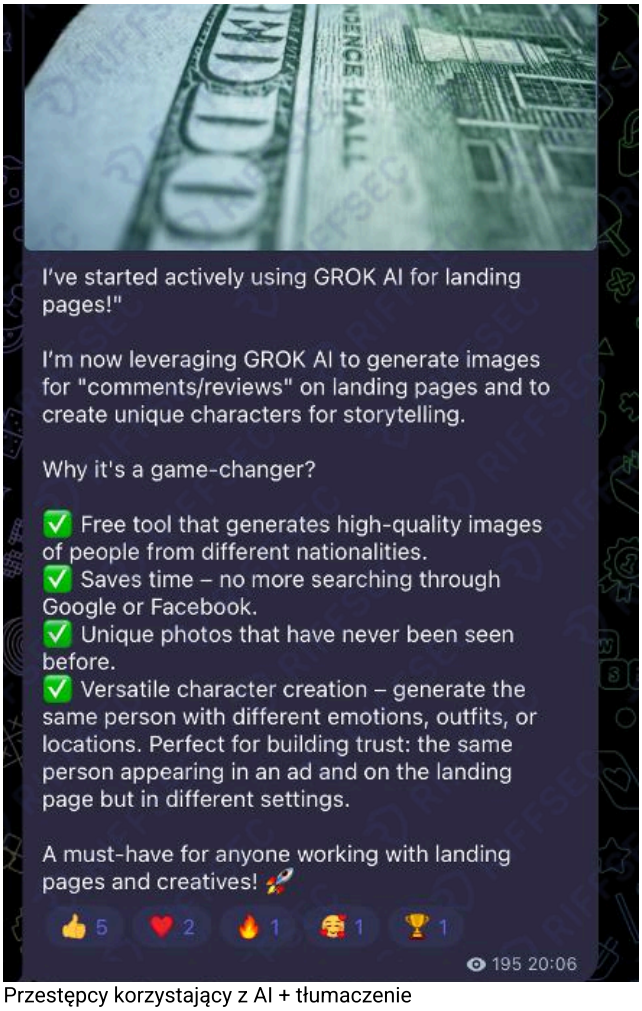
Ogłoszenie przestępcze o sprzedaży leadów



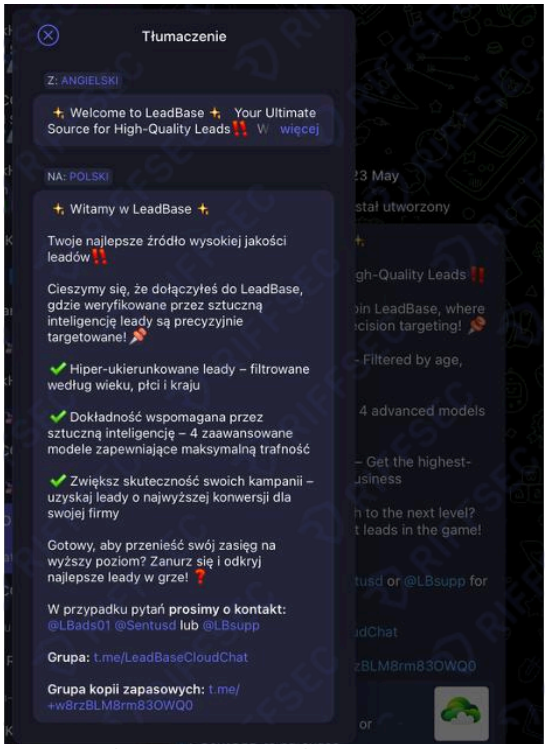
Ogłoszenie przestępcze o sprzedaży leadów

W niektórych ofertach przestępcy wskazują również na rozszerzony zakres informacji przypisanych do pojedynczego lead'a. Oprócz podstawowych danych kontaktowych mogą być tam zawarte dodatkowe informacje dotyczące potencjalnej ofiary, pozyskane między innymi na podstawie ogólnodostępnych źródeł (OSINT).

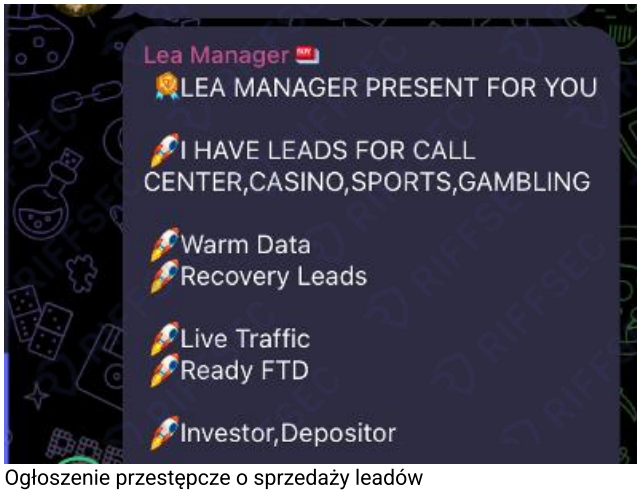
W niektórych ofertach przestępcy deklarują również wykorzystanie narzędzi sztucznej inteligencji do bardziej precyzyjnego profilowania i ukierunkowania leadów.
Ma to według nich zwiększać skuteczność kampanii oraz ułatwiać dopasowanie przekazu do potencjalnych ofiar. Narzędzia te są również wykorzystywane do generowania treści i narracji publikowanych na stronach pre-landingowych.



Przestępcy korzystający z AI + tłumaczenie



Przestępcy korzystający z AI + tłumaczenie



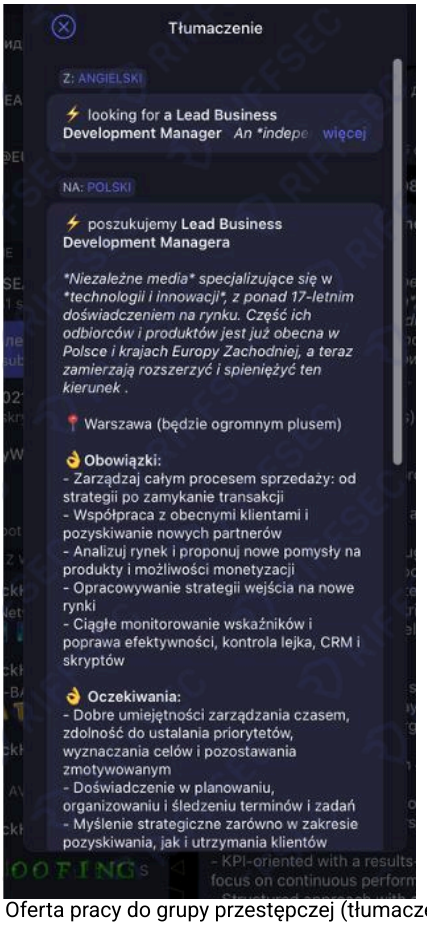
Ogłoszenie przestępcze o sprzedaży leadów

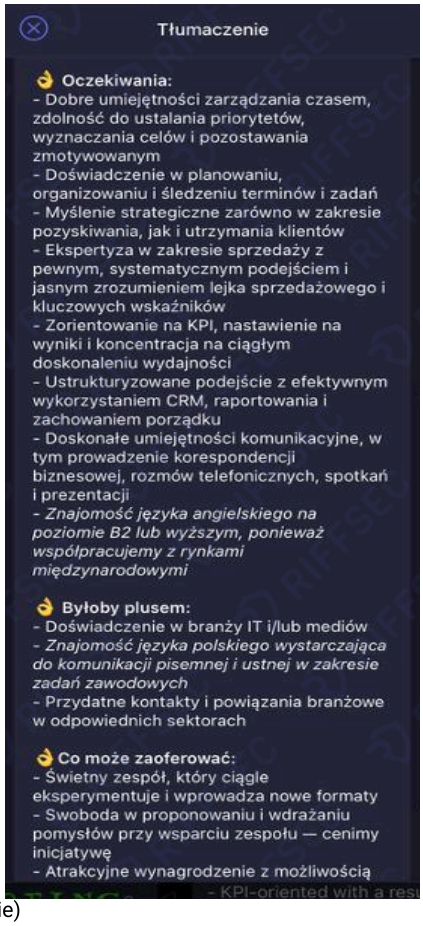
W sytuacji, gdy sprzedaż leadów związanych z jednym schematem przestępczym okazuje się niewystarczająca, niektóre grupy rozszerzają zakres swojej działalności. W takich przypadkach oferują na sprzedaż również leady pochodzące z innych scenariuszy przestępczych.

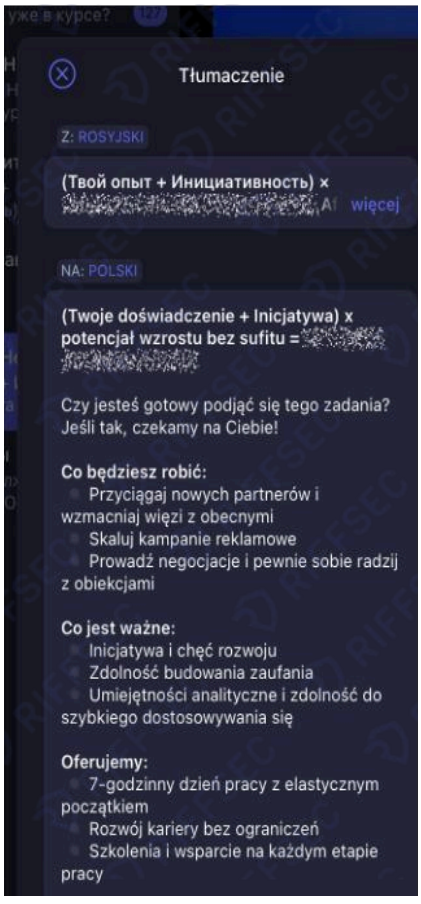
Rozwój rynku sprzedaży leadów sprawił, że działalność przestępcza w tym obszarze zaczęła przyjmować coraz bardziej zorganizowaną i profesjonalną formę. W odpowiedzi na rosnącą konkurencję oraz wymagania rynku oszuści zajmujący się pozyskiwaniem i sprzedażą danych zaczęli rozwijać bardziej rozbudowane struktury organizacyjne. W raporcie określamy jejako tzw. „korporacje leadowe".

Funkcjonowanie takich struktur wymaga zaangażowania wielu osób wykonujących różne zadania. W efekcie zaczęły powstawać przestępcze struktury organizacyjne przypominające klasyczne przedsiębiorstwa, wraz z podziałem ról i odpowiedzialności.

Wzrost liczby tego typu korporacji doprowadził do rosnącej konkurencji pomiędzy nimi, co z kolei spowodowało intensyfikację działań rekrutacyjnych. Pojawiły się liczne ogłoszenia dotyczące „zatrudnienia". Wśród oferowanych ról można znaleźć między innymi stanowiska określane jako Lead Business Development Manager, czy Media Buyer. Od przestępców pełniących tę pierwszą funkcję oczekuje się





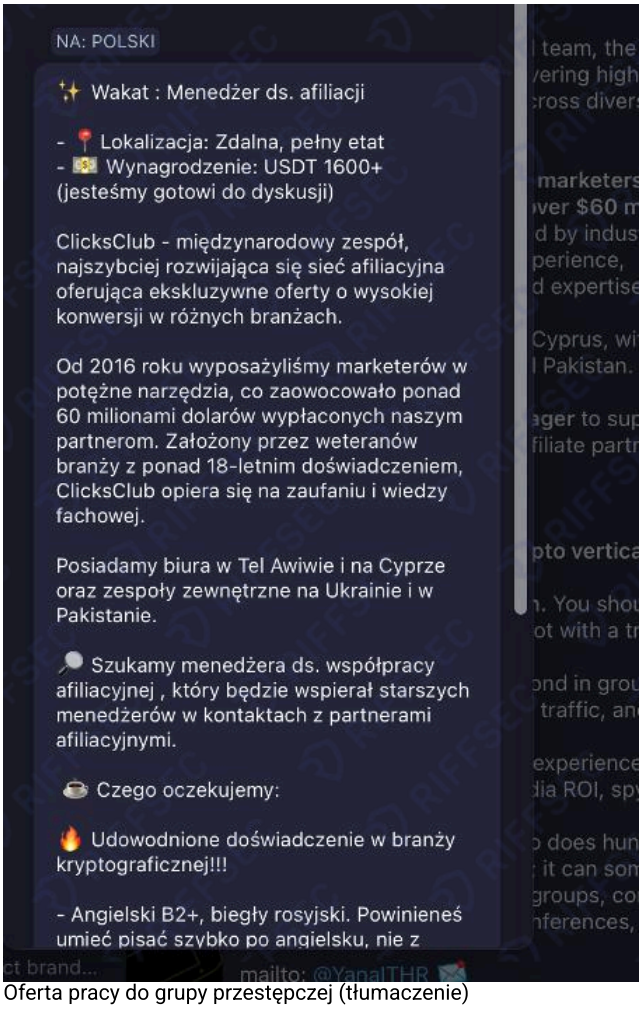


Oferta pracy do grupy przestępczej (tłumaczenie)

między innymi zarządzania procesem sprzedaży lead'ów, analizy rynku oraz identyfikowania potrzeb potencjalnych odbiorców, a także ustalania i monitorowania wskaźników efektywności oraz optymalizacji prowadzonych działań.

Innym przykładem tworzonego w tych strukturach stanowiska jest menedżer ds. afiliacji. Osoba pełniąca taką rolę odpowiada między innymi za analizę skuteczności kampanii reklamowych oraz ocenę, które kreacje marketingowe przynoszą najlepsze rezultaty. Do jej zadań należy również identyfikowanie grup odbiorców, do których reklamy trafiają najskuteczniej, a także analizowanie zachowania użytkowników w zakresie reagowania na określone treści reklamowe. Z perspektywy przestępczej działania te mają na celu zwiększenie liczby kliknięć w reklamy oraz pozyskanie jak największej liczby potencjalnych ofiar.

W ogłoszeniach tego typu często wskazywane jest również miejsce wykonywania pracy lub możliwość pracy zdalnej. Rekrutrzy (przestępcy) starają się uwiarygodnić ofertę, podkreślając rzekome doświadczenie grupy w prowadzeniu tego rodzaju działalności oraz współpracę z „partnerami biznesowymi". W rzeczywistości chodzi o inne grupy przestępcze, w tym struktury prowadzące przestępcze call center.

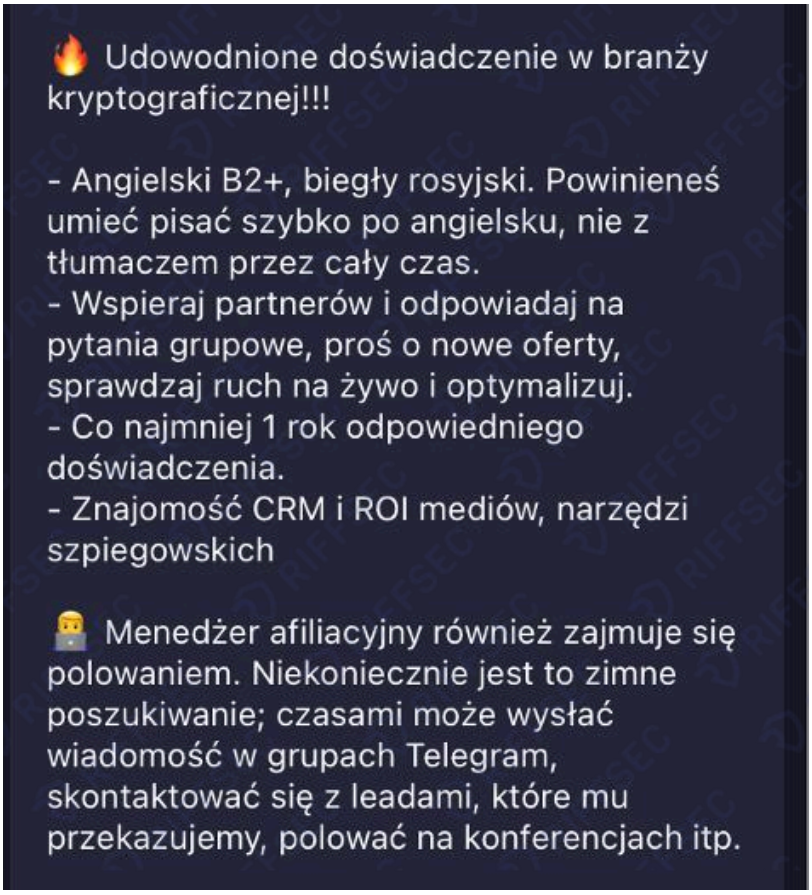


Oferta pracy do grupy przestępczej (tłumaczenie)

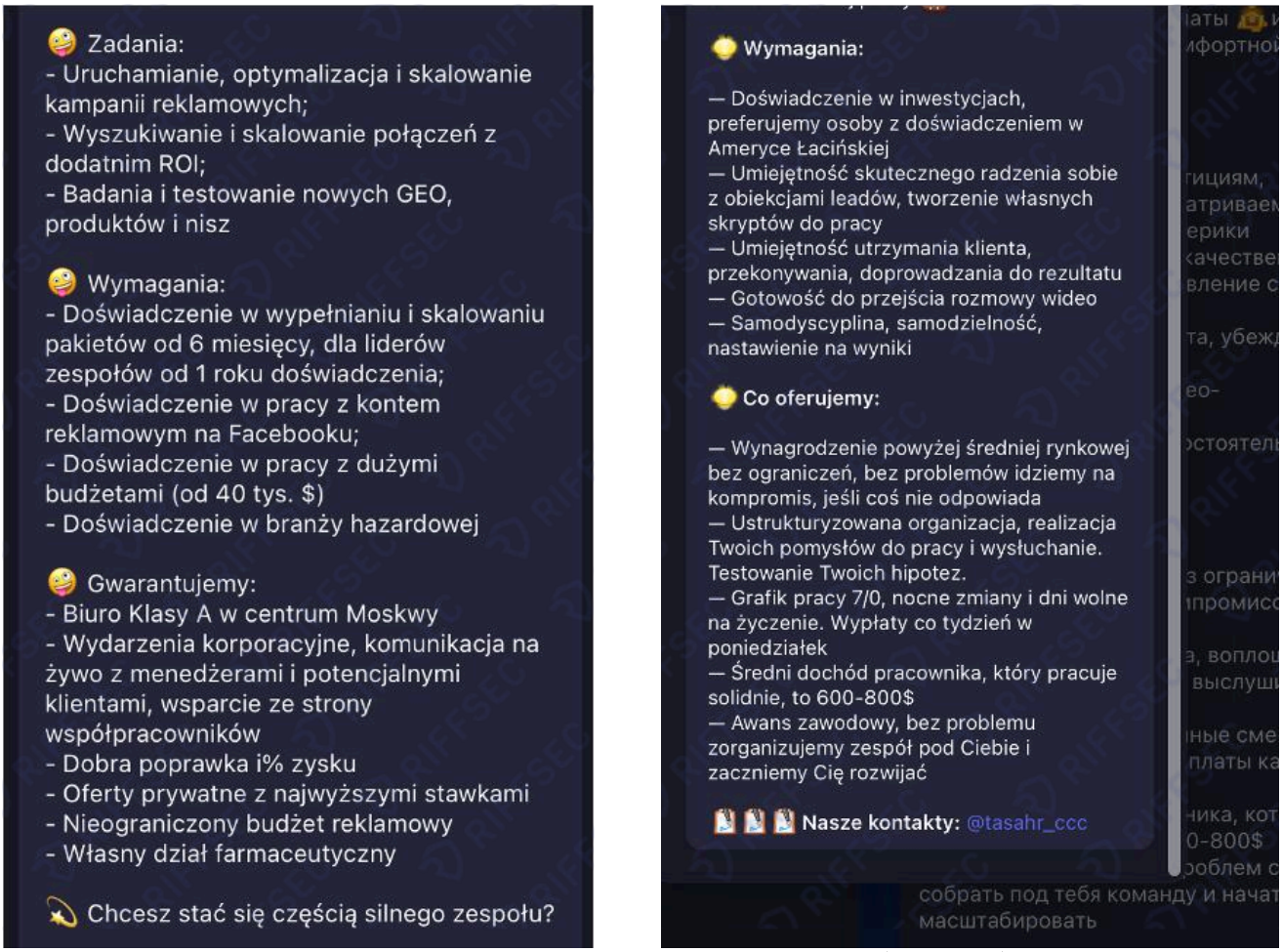
W przekazie rekrutacyjnym akcentowane jest także zapewnienie stabilnych i regularnych wypłat wynagrodzenia. Ma to stworzyć wrażenie funkcjonowania w ramach uporządkowanej organizacji oraz zachęcić potencjalnych kandydatów do zaangażowania się w działalność przestępczą.

Niektóre grupy przestępcze wprowadzają jeszcze bardziej szczegółowy podział ról. W takich przypadkach menedżer ds. afiliacji odpowiada przede wszystkim za zarządzanie siecią afiliacyjną, czyli organizowanie i nadzorowanie dystrybucji reklam w Internecie. Natomiast za analizę i przygotowanie samych kreacji reklamowych odpowiada menedżer ds. reklamy.

Do jego zadań należy między innymi określanie, pod czyj wizerunek się podszyć, gdzie publikować materiały reklamowe, a także jakie tematy i narracje mogą być najbardziej skuteczne w danym kraju.



Oferta pracy do grupy przestępczej (tłumaczenie)

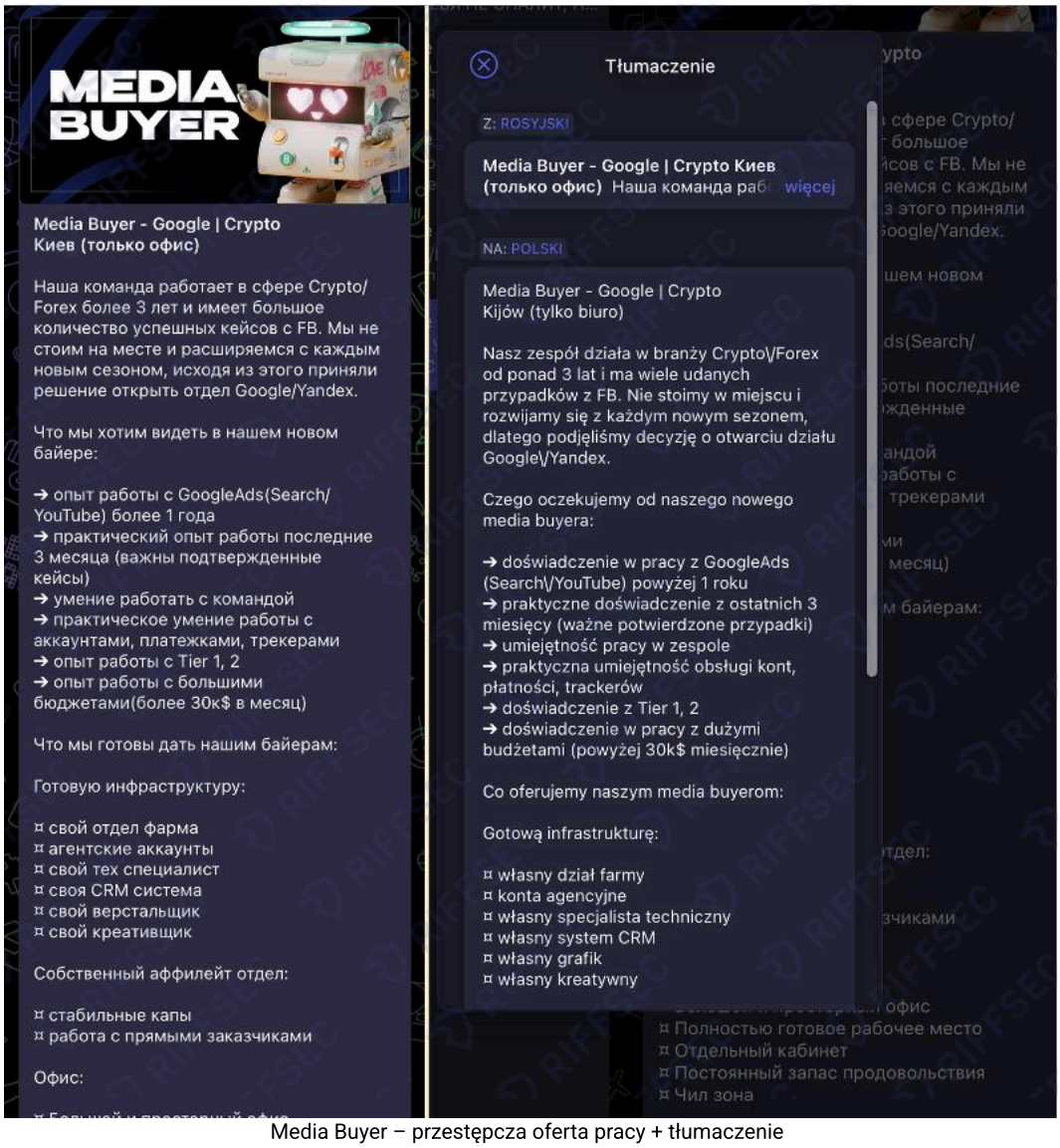


Przykładowe zadania i wymagania w przestępczych ofertach pracy (tłumaczenie)

W strukturach tych organizacji pojawia się również rola określana jako Media Buyer. Zadaniem osoby pełniącej taką funkcję jest analizowanie oraz optymalizowanie sposobów zakupu reklam na różnych platformach internetowych, takich jak Facebook, TikTok czy Google. Celem tych działań jest maksymalizacja skuteczności kampanii przy jednoczesnym ograniczaniu ryzyka wykrycia przez mechanizmy bezpieczeństwa platform reklamowych.

Do obowiązków tej osoby może należeć także pozyskiwanie zasobów wykorzystywanych do prowadzenia kampanii reklamowych. W praktyce oznacza to między innymi zakup baz danych, takich jak dane kart płatniczych, lub przejmowanie gotowych kont w mediach społecznościowych, do których przypisane są metody płatności należące do ofiar innych przestępstw.

W scenariuszu fałszywych inwestycji tzw. korporacje leadowe często wykorzystują właśnie takie konta do publikowania reklam. Działanie to ma zwiększyć wiarygodność profilu, z którego publikowane są materiały reklamowe, oraz utrudnić ich szybkie zidentyfikowanie jako elementu działalności przestępczej.



Media Buyer – przestępcza oferta pracy + tłumaczenie

Warto podkreślić, że za każdym z opisanych stanowisk bardzo często stoi cały zespół osób realizujących określone zadania. Osoby te mają wyznaczone obowiązki, terminy realizacji oraz cele do osiągnięcia. Podlegają również procesom zarządzania, są rozliczane z efektów swojej pracy, motywowane do zwiększania wyników, a w razie potrzeby także zastępowane lub usuwane ze struktur organizacji.

Należy przy tym pamiętać, że cały czas mowa o funkcjonowaniu zorganizowanych grup przestępczych. Liczba ról i stanowisk występujących w takich strukturach jest w rzeczywistości znacznie większa niż te opisane powyżej.

Ogłoszenie przestępcze o sprzedaży ledów subskrypcyjnym wskazuje, że istnieje również druga strona tego mechanizmu. Oznacza to, że podmioty oferujące tego typu usługi mają swoich odbiorców, którzy kupują pozyskane dane i wykorzystują je w dalszych etapach przestępczego schematu.

Korporacje telefoniczne (call center)

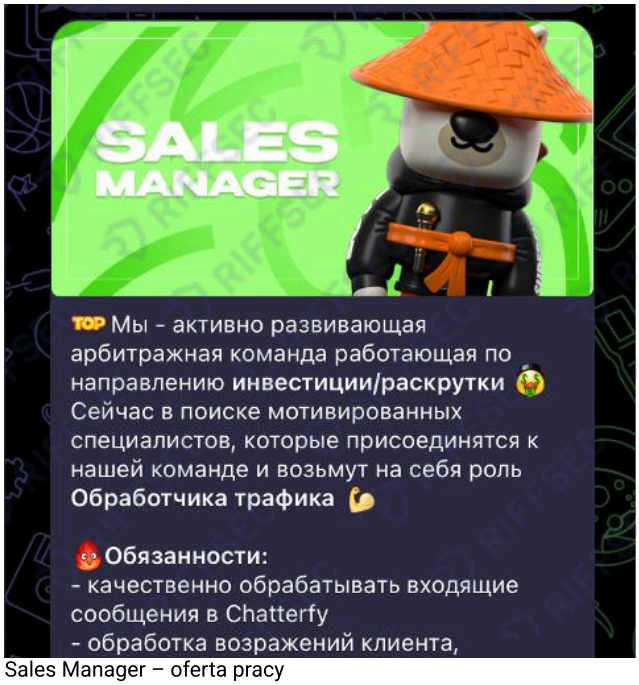
Kolejnym elementem tego ekosystemu przestępczego są tzw. korporacje telefoniczne, czyli struktury działające w formie przestępczych call center. Tego typu organizacje powstały znacznie wcześniej niż korporacje leadowe i odpowiadają za bezpośredni kontakt z ofiarami. To właśnie osoby pracujące w takich strukturach prowadzą rozmowy telefoniczne z potencjalnymi ofiarami, stosują opisane wcześniej techniki manipulacyjne oraz bezpośrednio doprowadzają do wyłudzenia środków finansowych. W praktyce oznacza to, że są one odpowiedzialne za realizację końcowego etapu oszustwa.

Struktury te są często jeszcze bardziej rozbudowane organizacyjnie niż korporacje leadowe. Funkcjonują w oparciu o wyraźną hierarchię, w której poszczególne osoby mają określony zakres obowiązków. Dla części osób zaangażowanych w taką działalność jest to traktowane jak standardowe miejsce pracy. W przeciwieństwie do wielu działań związanych z pozyskiwaniem leadów, działalność przestępczych call center w dużej mierze odbywa się stacjonarnie. Grupy te organizują fizyczne przestrzenie pracy, w których osoby zaangażowane w proceder spotykają się codziennie o określonych godzinach. Praca ma często charakter zmianowy, a jej głównym celem jest prowadzenie rozmów z potencjalnymi ofiarami i nakłanianie ich do przekazywania środków finansowych.

Podobnie jak w przypadku poprzednich struktur przestępczych, również tutaj rozwój organizacji zależy od liczby zaangażowanych osób. Z tego powodu grupy te prowadzą intensywne działania rekrutacyjne i starają się konkurować z innymi organizacjami przestępczymi o nowych „pracowników". Najbardziej podstawową i jednocześnie najliczniej obsadzaną rolą w takich strukturach są osoby wykonujące telefoniczne do potencjalnych ofiar. Określane są one często jako operatorzy lub telefoniści. Od kandydatów na takie stanowiska oczekuje się przede wszystkim znajomości języka używanego w kraju, do którego kierowany jest atak, a także doświadczenia w prowadzeniu rozmów sprzedażowych lub w realizacji określonych scenariuszy oszustw.

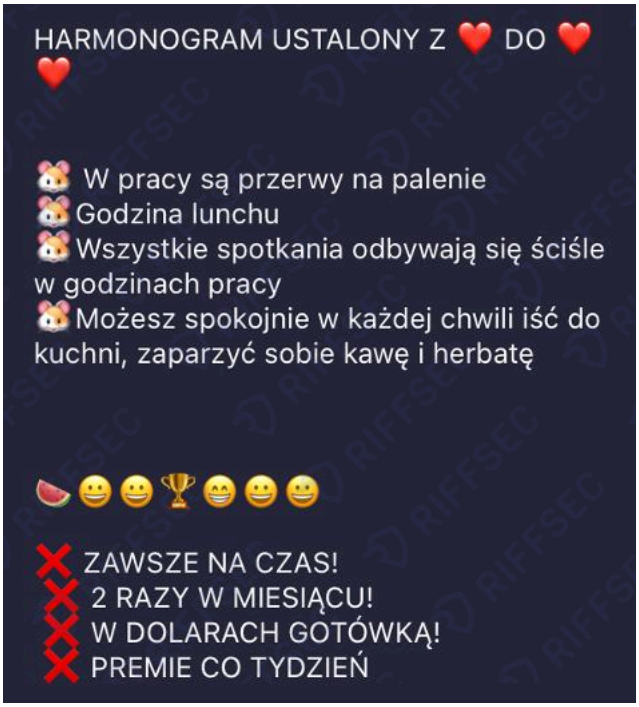
W celu przyciągnięcia nowych osób do pracy przestępcze call center oferują regularne wypłaty wynagrodzenia oraz liczne benefity. Mowa tutaj m.in. o imprezach integracyjnych, czy konkursach efektywności z nagrodami rzeczowymi np. najnowsze modele laptopów Apple). Warto jednak zwrócić uwagę, że „efektywność" w tym wypadku to liczba oszukanych osób lub kwota na jaką udało się okraść ofiary.

Ogłoszenia podkreślają również atrakcyjną lokalizację biur oraz warunki pracy. W materiałach rekrutacyjnych można znaleźć szczegółowe informacje dotyczące organizacji dnia pracy, w tym godzin rozpoczęcia i zakończenia zmian, przerw na posiłki czy zasad korzystania z przerw w trakcie dnia.

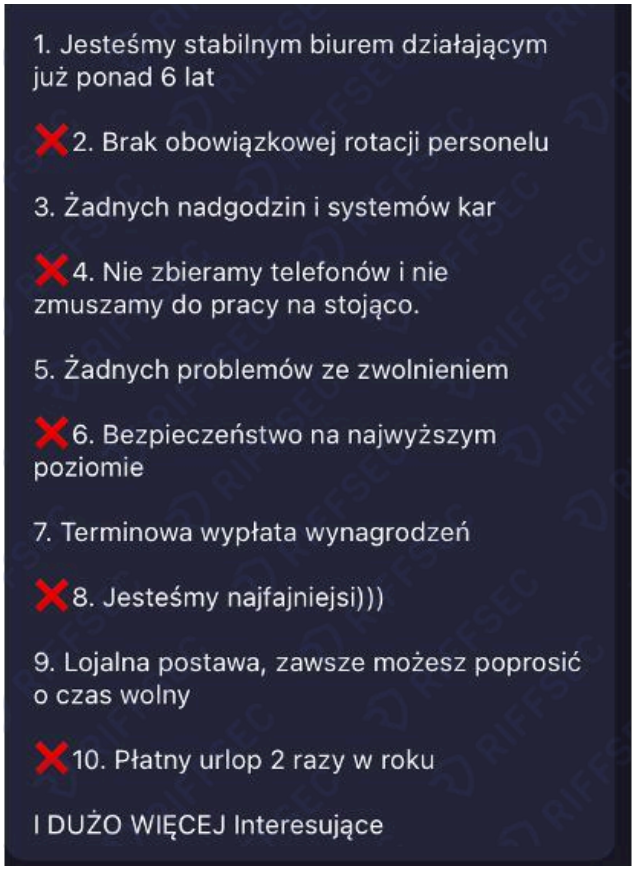


Sales Manager – oferta pracy

W niektórych przypadkach, szczególnie po rozpoczęciu pełnoskalowej agresji Rosji na Ukrainę, pojawiały się także deklaracje dotyczące zapewnienia pracownikom możliwości schronienia w miejscu pracy, niekiedy wraz z częścią członków ich rodzin. Tego rodzaju komunikaty miały na celu zwiększenie atrakcyjności oferty i zachęcenie do podjęcia pracy w strukturach przestępczych.



Przykładowe warunki i zasady pracy w przestępczym call centre (tłumaczenie)



Przykładowe warunki i zasady pracy w przestępczym call centre (tłumaczenie)

W strukturach przestępczych call center zespoły pracowników są zazwyczaj nadzorowane przez liderów lub menedżerów zespołów. Osoby te odpowiadają za koordynację pracy operatorów, monitorowanie wyników oraz realizację założonych celów.

Stanowiska te mogą być obsadzane zarówno poprzez „awans" oszustów już działających w strukturach danej grupy, jak i poprzez rekrutację zewnętrzną. W środowiskach przestępczych pojawiają się również ogłoszenia dotyczące poszukiwania kandydatów na tego typu funkcje.

W ramach takich struktur zespoły często konkurują między sobą o wyniki osiągane w prowadzonej działalności. Rywalizacja polega przede wszystkim na osiąganiu jak najwyższych rezultatów, rozumianych jako liczba pozyskanych ofiar lub wysokość wyłudzonych środków.

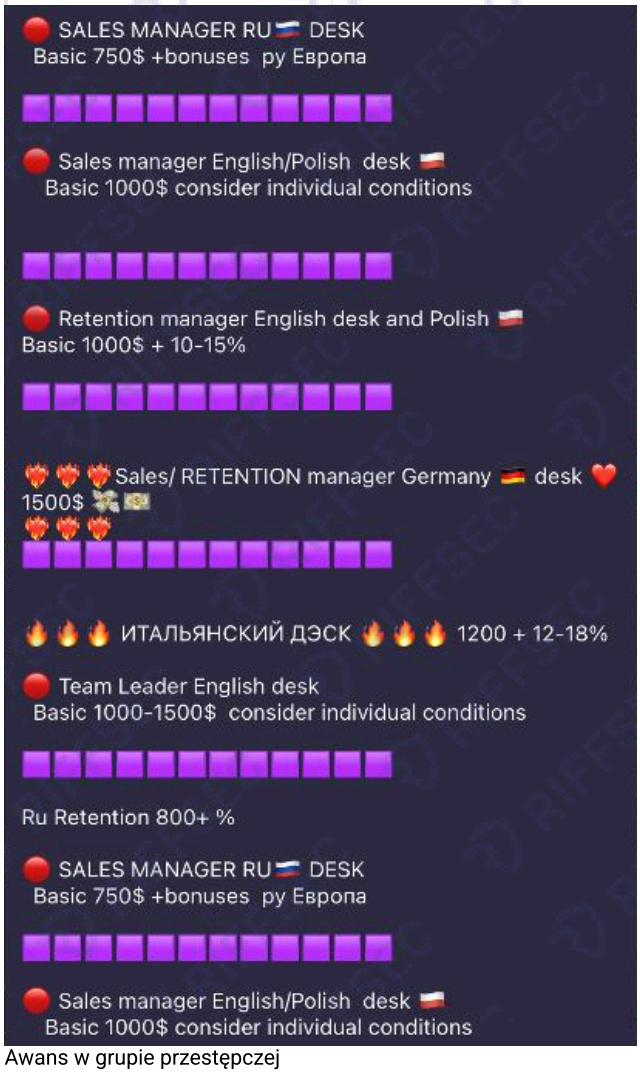
Oferta pracy lidera zespołu

Najlepsze zespoły w określonych okresach rozliczeniowych, na przykład tygodniowych, mogą otrzymywać dodatkowe nagrody lub formy motywacji. W materiałach rekrutacyjnych pojawiają się informacje o różnego rodzaju benefitach, takich jak finansowanie posiłków dla zespołu (Pizza Day) czy inne nagrody przyznawane „na koszt firmy".

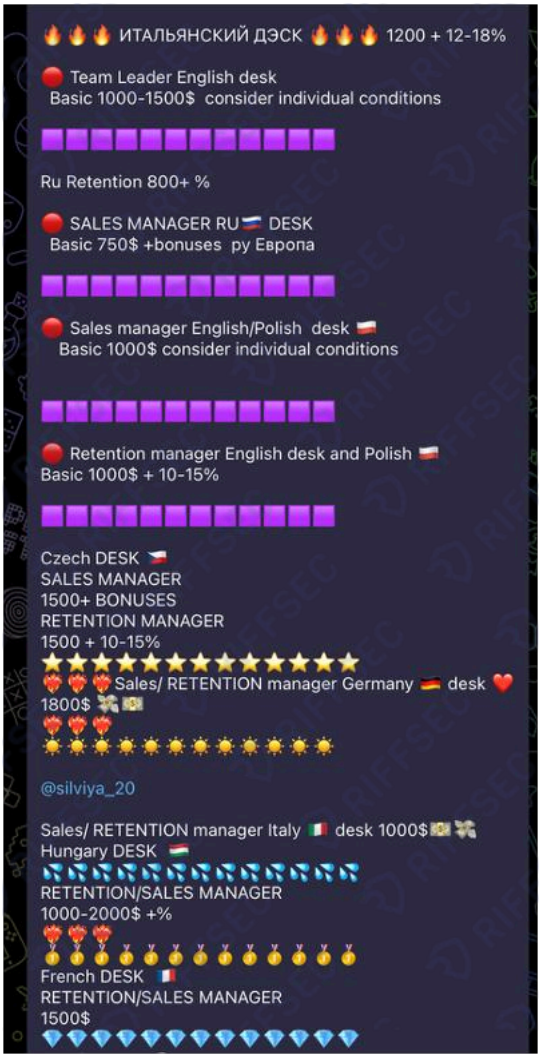
W strukturach przestępczych call center wykształciły się również swoiste „ścieżki kariery". Poszczególne role są jasno określone, a osoby zaangażowane w działalność tych struktur wiedzą, jakie stanowiska mogą osiągnąć w kolejnych etapach swojej aktywności. Awans w takich organizacjach jest najczęściej powiązany z osiąganymi wynikami, w szczególności z wysokością wyłudzonych środków lub skutecznością w prowadzeniu rozmów z ofiarami. Przejście na wyższe stanowiska oczywiście związane jest ze wzrostem poziomu wynagrodzenia oraz zakresu odpowiedzialności.

Przykładowe warunki i zasady pracy w przestępczym call center (tłumaczenie)

W efekcie osoby zaangażowane w tego typu działalność funkcjonują w strukturze przypominającej klasyczną hierarchię zawodową, w której kolejne stanowiska i poziomy zarobków stanowią motywację do dalszego działania w ramach przestępczej organizacji.

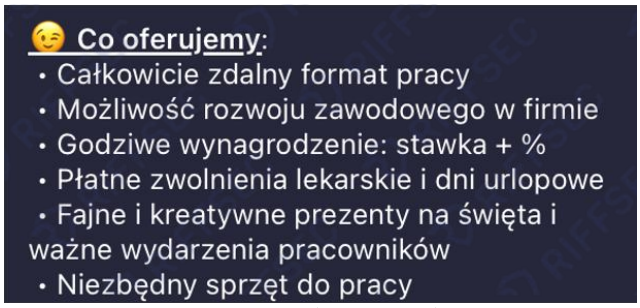


Awans w grupie przestępczej



Awans w grupie przestępczej

Jednym z bardziej zaskakujących przykładów benefitów oferowanych w tego typu strukturach jest wprowadzenie (stosunkowo niedawno i nie we wszystkich grupach) płatnego zwolnienia lekarskiego. Tego rodzaju rozwiązanie jest prezentowane jako dodatkowy element motywacyjny mający zwiększyć atrakcyjność „zatrudnienia".



Płatne L4 w grupie przestępczej (tłumaczenie)

Jednocześnie osoby zarządzające takimi strukturami podkreślają, że zwolnienia lekarskie będą weryfikowane i nie będą tolerowane próby ich nadużywania. W praktyce oznacza to, że również w środowisku przestępczym pojawiają się mechanizmy kontroli mające zapobiegać sytuacjom, w których członkowie organizacji nadużywają oferowanych przywilejów (bo przestępcy oszukują przestępców).

Wysokość wynagrodzenia oferowanego w przestępczych call center często zależy również od rynku, na który kierowane są działania. W ogłoszeniach rekrutacyjnych można zauważyć, że stawki różnią się w zależności od kraju, w którym prowadzone są oszustwa oraz języka, w którym prowadzone będą rozmowy z ofiarami.

Rozbudowane struktury organizacyjne tych grup powodują również konieczność prowadzenia stałej rekrutacji nowych osób. W związku z tym w ramach takich organizacji powstają wyspecjalizowane zespoły odpowiedzialne za procesy rekrutacyjne, pełniące funkcję zbliżoną do działów HR. W odpowiedzi na zapotrzebowanie rynku przestępczego pojawiły się także mniejsze grupy, które specjalizują się wyłącznie w wyszukiwaniu, weryfikowaniu oraz pozyskiwaniu nowych osób do pracy w przestępczych strukturach.

Osoby dopiero rozpoczynające działalność w takich organizacjach, które nie posiadają wcześniejszego doświadczenia lub nie znają konkretnego scenariusza oszustwa, przechodzą szkolenia organizowane przez daną grupę. W celu zwiększenia atrakcyjności oferty niektóre organizacje deklarują również wynagrodzeniez a czas poświęcony na szkolenie.

Interesującym z analitycznego punktu widzenia stanowiskiem w takich strukturach są również osoby odpowiedzialne za kontrolę jakości prowadzonych rozmów. Do ich zadań należy odsłuchiwanie nagrań rozmów prowadzonych przez operatorów z ofiarami. Warto zaznaczyć, że w wielu przypadkach same grupy przestępcze rejestrują część prowadzonych połączeń. Na podstawie tych nagrań przygotowywane są analizy dotyczące zarówno sposobu prowadzenia rozmowy przez konkretnego operatora, jak i skuteczności stosowanego scenariusza manipulacji. Wnioski z takich analiz są następnie przekazywane osobom zarządzającym strukturą, czyli organizatorom działalności przestępczej.

Na tej podstawie wprowadzane są dalsze zmiany w sposobie działania, w tym modyfikacje scenariuszy rozmów z ofiarami lub decyzje personalne dotyczące osób prowadzących rozmowy.

Stanowisk, oferowanych benefitów, wymagań rekrutacyjnych, stosowanych technik socjotechnicznych oraz sposobów działania przestępców jest w rzeczywistości znacznie więcej. Przedstawione powyżej przykłady mają jednak pokazać skalę oraz poziom organizacji tego zjawiska. Opisane mechanizmy dowodzą, że nie mamy do czynienia z pojedynczymi osobami działającymi w odosobnieniu. W rzeczywistości są to zorganizowane, hierarchiczne struktury przestępcze, które funkcjonują w sposób przemyślany i stale rozwijany.

Grupy te systematycznie optymalizują swoje działania, analizują skuteczność stosowanych metod oraz dostosowują je do zmieniających się warunków. W efekcie każdego dnia prowadzą działania w wielu krajach jednocześnie, wyłudzając od swoich ofiar znaczne środki finansowe. Oznacza to też, że każdy z nas może stać się celem ich działania. Kluczowe zatem staje się pytanie, jak rozpoznać, że znaleźliśmy się w takiej sytuacji oraz ograniczyć ryzyko zanim zostaniemy oszukani.

Jak o siebie i innych zadbać

Po pierwsze pamiętajmy, że jeżeli oferta jest zbyt piękna to prawdopodobnie będzie oznaczać, że jest nieprawdziwa, a na pewno potrzebuje dokładnej analizy. Jeżeli coś nas zainteresuje dajmy sobie czas żeby pomyśleć, poszukać informacji, skonsultować z osobami trzecimi (nie powiązanymi z „inwestycją"). Legalne inwestycje nie wymagają decyzji w kilka minut. Dodatkowo, jeżeli twarzą inwestycji jest znany polityk lub celebryta to prawdopodobnie jest to oszustwo ponieważ politycy nie mogą reklamować produktów inwestycyjnych, a celebryci robią to bardzo rzadko.

- Nie istnieje coś takiego jak gwarantowany wysoki zysk bez ryzyka. W inwestycjach nie ma gwarancji i ryzyko zawsze występuje. Dodatkowo żadna legalna strona inwestycyjna nie będzie wymagać od Ciebie podania tylko imienia, telefonu i adres e-mail żeby się skontaktować. Proces zakładania konta maklerskiego jest znacznie dłuższy i znacznie bardziej skomplikowany.

- Jeśli czegoś nie rozumiesz, nie inwestuj. Jeżeli nie znasz się na inwestowaniu to wszelkiego rodzaju informacji zasięgnij w stacjonarnym oddziale zweryfikowanej firmy inwestycyjnej. Brak możliwości przyjścia do biura/oddziału firmy to ważny sygnał ostrzegawczy – profesjonalne firmy inwestycyjne to nie „krzaki" załatwiające wszystko przez komunikator czy e-mail.

- Jeżeli już postanowimy zainwestować, to korzystajmy tylko ze znanych i zweryfikowanych podmiotów inwestycyjnych. Skontaktujmy się z ich przedstawicielem sami, nie czekajmy na telefon od „doradcy inwestycyjnego". Jednocześnie do kontaktu wykorzystując z oficjalne kanały komunikacji. Legalne firmy inwestycyjne nigdy nie korzystają z komunikatorów do kontaktu ze swoimi klientami, szczególnie w sprawach operacji finansowych.

- Nie dawaj dostępu do komputera osobie trzeciej, pod pretekstem „pomocy". Udostępnianie zawartości swoje pulpitu komuś, kogo nie znamy i nie możemy zweryfikować, może skończyć się bardzo źle. Nie wykonuj przelewów na zlecenie telefoniczne i nie realizuj próśb o wykonanie przelewu w formie maila lub informacji tekstowej na komunikatorze.

A jeżeli już się stanie, i Ty lub ktoś z Twojego otoczenia da się oszukać, to jak najszybciej zadzwoń do banku i zabezpiecz te dane, które mogą mieć przestępcy. Pamiętaj też o złożeniu zawiadomienia na policji, o podejrzeniu popełnienia przestępstwa i przekazaniu jak najbardziej szczegółowych informacji dotyczących m.in kanałów kontaktów z przestępcami, rachunków na które wpłacane były środki finansowe itd..

Warto też śledzić informacje o tym jak oszukują przestępcy. Czytać, dowiadywać się, a nawet pytać, znając sposoby ich działania istnieją większe szanse, że będziemy w stanie rozpoznać niebezpieczne zachowania. A jak już wiemy, to informujmy dalej, mówimy o tym i ostrzegajmy, nie ma skuteczniejszej drogi, niż „poczta pantoflowa".

Adam Haertle

Twórca i redaktor naczelny serwisu zaufanatrzeciastrona.pl

Kilka lat temu obawiałem się, że kiedyś nie będę już mógł nadążyć za nowymi technikami przestępców. Cyberprzestępcy tworzyli coraz bardziej zaawansowane konie trojańskie, firmy antywirusowe pisały coraz bardziej wyrafinowane narzędzia wykrywające złośliwe oprogramowanie i wydawało się, że wyścig technologiczny nie będzie miał końca.

Tymczasem okazało się, że trend się w dużym stopniu odwrócił i przestępcy odkryli, że techniki manipulacji są dużo prostsze w użyciu niż skomplikowane narzędzia IT. Wystarczy znaleźć pracowników bez skrupułów, przeszkolić ich we właściwym prowadzeniu konwersacji z ofiarami, wykupić reklamy w mediach społecznościowych i przygotować systemy prania skradzionych środków. Hakowanie mózgów jest paradoksalnie prostsze, ponieważ nikt do tej pory nie wyprodukował antywirusa, którego możemy zainstalować w głowach naszych rodziców czy dziadków.

Proste techniki manipulacji takie jak żądza zysku czy presja czasu pozwalają ofiarom zapomnieć o własnym rozsądku i ostrzeżeniach, a przestępcy niezwykle łatwo potrafią wpływać na decyzje swoich ofiar, korzystając z gotowych skryptów i instrukcji. To powoduje, że osoby skuszone niebotycznymi zyskami oddają często wszystkie swoje oszczędności, a czasem nawet zadłużają się, by nie przegapić „świetnych okazji". Do tego przestępcy często operują z zagranicy, co powoduje, że zjawisko to jest ogromnym wyzwaniem dla organów ścigania.

Co możemy zrobić? Dopilnujmy, by wszyscy nasi bliscy mieli zastrzeżony PESEL i opowiadajmy im przy każdej okazji historie oszustw – zwiększamy w ten sposób szansę, że zorientują się, gdy to do nich zadzwoni „doradca inwestycyjny".

Maciej Broniarz

DC9 CYBER

Skala i niestety skuteczność oszustw inwestycyjnych pokazują, że zabezpieczenia techniczne to za mało, żeby zapewnić bezpieczeństwo użytkownikom internetu i ich portfelom.

Co gorsza, rozwój narzędzi wykorzystujących AI daje dodatkowe możliwości przestępcom i znacząco ułatwia im pracę. Musimy pamiętać, że za oszustwami tego typu nie stoją pojedyńcze osoby oszukujące swoje ofiary z zacisza domowej piwnicy, ale duże i profesjonalnie działające firmy, których celem jest masowe, skuteczne i pozbawione skrupułów oszukiwanie i okradanie ludzi. Skala i niestety skuteczność oszustw inwestycyjnych pokazują, że zabezpieczenia techniczne to za mało, żeby zapewnić bezpieczeństwo użytkownikom internetu i ich portfelom.

W dobie ataków typu human-centric, gdzie celem nie jest luka w oprogramowaniu, lecz emocje ofiary, technologia staje się jedynie tłem dla wyrafinowanej inżynierii społecznej. Co gorsza, rozwój narzędzi wykorzystujących AI, takich jak zaawansowane deepfake'i czy zautomatyzowane boty konwersacyjne, daje przestępcom dodatkowe możliwości i znacząco ułatwia im skalowanie procederu.

Musimy pamiętać, że za oszustwami tego typu nie stoją pojedyncze osoby działające z zacisza domowej piwnicy, ale profesjonalnie zorganizowane grupy przestępcze – swoiste „fabryki oszustw", dysponujące strukturą korporacyjną, działami IT i ogromnymi budżetami marketingowymi. Ich celem jest masowe i pozbawione skrupułów okradanie ludzi, często przy wykorzystaniu platform społecznościowych jako głównego kanału dystrybucji.

Bez połączenia technologii, restrykcyjnej moderacji treści przez gigantów technologicznych oraz wysokiej świadomości społecznej, problemu nie tylko nie da się wyeliminować, ale będzie on stale narastać.

Krzysztof Zieliński

CISO RTV EURO AGD

Opisywany w raporcie scenariusz przestępczy rozwija się skutecznie od wielu lat. Jego nowe odsłony, wykorzystujące technologię deepfake'ów, pokazują, że przestępcy odnaleźli w tej formie oszustwa zarówno łatwość działania, jak i wysoką dochodowość.

Skuteczność tego rodzaju oszustw wynika z wielu aspektów - niskiej świadomości społecznej w zakresie cyberzagrożeń, braku podstawowej wiedzy finansowej, braku krytycznego myślenia, klasycznego FOMO, naiwności oraz łatwowierności wspartej chęcią szybkiego wzbogacenia się. Te cechy ludzkiej psychiki, obecne od zarania dziejów, były i są przez przestępców wykorzystywane na różnych polach działalności, a Internet stał się kolejnym obszarem tego typu praktyk. Jednak w odróżnieniu od klasycznych, analogowych „wektorów ataku", Internet, dzięki swoim cechom, zapewnia najszerszą w dotychczasowej historii ludzkości drogę dotarcia do ofiar, dodatkowo oferując przestępcom wysoki poziom anonimowości.

Niezależnie od powodów takiego, a nie innego działania użytkowników Internetu, u podstaw tego oszustwa leży reklama publikowana na portalach internetowych i w mediach społecznościowych. Oficjalna reklama działań przestępczych (!), która jest powszechnie dostępna, czy wręcz celowo wyświetlana użytkownikom przez algorytmy zarządzające reklamami, stanowi kluczowy element tego scenariusza. Właśnie w powszechnej dostępności takich reklam należy upatrywać skuteczności tego konkretnego scenariusza przestępczego. Można twierdzić, że jest to słabość przepisów prawa i ich egzekwowania; pamiętajmy jednak, że prawo zazwyczaj podąża za technologią, a stosowne przepisy są wprowadzane w odpowiedzi na zmieniającą się rzeczywistość.

Unia Europejska wprowadziła w 2024 r. przepisy sankcjonujące dystrybucję nielegalnych treści w Internecie w ramach Dyrektywy DSA. Polska implementacja DSA jest na etapie prac legislacyjnych od września 2025 r., tj. rok po wejściu w życie dyrektywy. Sprawność procesów legislacyjnych w Polsce pozostawia wiele do życzenia, co wielokrotnie widzieliśmy chociażby w przypadku implementacji dyrektywy NIS2. Wybór UKE na organ nadzorczy odpowiedzialny za egzekwowanie przepisów DSA w Polsce również stawia pod znakiem zapytania skuteczność ich realizacji. Wiedza, kompetencje i zasoby niezbędne do spełnienia tych zadań nie leżą gotowe do wykorzystania - trzeba je zbudować od podstaw, co zajmie sporo czasu.

Niezależnie od przepisów prawa i ich egzekwowania największą bolączką jest całkowity brak cyberodpowiedzialności po stronie dostawców treści w Internecie. Dla przykładu Meta (właściciel Facebooka) od 2020 r. szeroko komunikuje o kolejnych algorytmach i procesach, które mają zabezpieczyć użytkownika przed zalewem treści niepożądanych - dezinformacji, deepfake, oszustw itd. Te zapowiedzi drastycznie rozmijają się z rzeczywistością. Facebook jest siedliskiem reklam fałszywych inwestycji nie tylko w przestrzeni polskich użytkowników. Reklamy tego typu są masowo serwowane na całym świecie, odpowiednio profilowane dla danej grupy odbiorców przez algorytmy FB.

Krzysztof Zieliński

CISO RTV EURO AGD

Zgłaszania tego typu treści jako szkodliwych jest nieskuteczne, FB w znaczącej większości przypadków nie usuwa ich. Podobnie dzieje się na innych platformach mediów społecznościowych. Google jako dostawca największej wyszukiwarki internetowej, mimo deklaracji ochrony swoich użytkowników, pozwala przestępcom umieszczać reklamy fałszywych inwestycji w Google Ads, czy też odpowiednio pozycjonować strony przestępcze. Czy problem ze skutecznym eliminowaniem treści przestępczych z Internetu jest trudny technicznie? W dobie modeli AI które odpowiednio wytrenowane są w stanie piekielnie dobrze realizować zaawansowane prace w zakresie analizy treści? Globalne korporacje o których mówimy mają do tego odpowiednie zasoby finansowe i techniczne. Czy więc brakuje woli i chęci bo czerpią niemałe korzyści finansowe z działalności przestępczej na swoich platformach? Bo przecież taka skala reklam generuje kolosalne przychody. To pytanie w formie otwartej pozostawiam czytelnikom do własnego przemyślenia.

RIFFSEC Sp. z o.o.

Pl. Bankowy 2

00-095 Warszawa

RIFFSEC

riffsec.com
@getriffsec