Michał Bukowski[1]
ORCID: 0000-0002-5075-8130

Zwalczanie cyberprzestępczości ekonomicznej przy wykorzystaniu sztucznej inteligencji (AI)

Wstęp

Europol[2] definiuje przestępczość finansową lub gospodarczą jako „przestępczość gospodarczą, zwaną również przestępstwem finansowym"[3]. Odnosi się ona do bezprawnych czynów popełnionych przez osobę lub grupę osób w celu uzyskania korzyści finansowej lub zawodowej, której głównym motywem jest zysk ekonomiczny (finansowy). Przestępczość tego rodzaju obejmuje m.in. pranie brudnych pieniędzy, uchylanie się od płacenia podatków, oszustwa inwestycyjne, oszustwa związane z marketingiem masowym oraz wiele innych. Przestępczość związaną z finansami Światowe Forum Ekonomiczne[4] wyceniło na ponad bilion dolarów. W chwili obecnej w Polsce funkcjonują trzy duże struktury organizacyjne związane ze zwalczaniem przestępczości ekonomicznej. Biuro Zwalczania Prze-

[1] Mł. insp. dr inż. Michał Bukowski — od 1997 r. funkcjonariusz Policji, od lipca 2023 r. dyrektor Instytutu Służby Kryminalnej Wydziału Bezpieczeństwa i Nauk Prawnych Akademii Policji w Szczytnie, wcześniej naczelnik Wydziału Techniki Operacyjnej Komendy Wojewódzkiej Policji w Gdańsku, naczelnik Wydziału Wsparcia Operacyjnego Biura Spraw Wewnętrznych Policji oraz zastępca naczelnika Wydziału Techniki Specjalnej i Realizacji Biura Kryminalnego Komendy Głównej Policji. Absolwent Polsko-Japońskiej Akademii Technik Komputerowych Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie oraz Wojskowej Akademii Technicznej.
Kontakt z autorem za pośrednictwem redakcji.

[2] Misją Europolu, który ma siedzibę w Hadze (Holandia), jest wspieranie państw członkowskich w zapobieganiu wszelkim formom poważnej przestępczości międzynarodowej i zorganizowanej, cyberprzestępczości i terroryzmowi oraz w ich zwalczaniu. Europol współpracuje także z wieloma państwami partnerskimi spoza UE oraz z organizacjami międzynarodowymi. Duże sieci przestępcze i terrorystyczne stanowią poważne zagrożenie dla bezpieczeństwa wewnętrznego UE oraz dla bezpieczeństwa i warunków życia jej mieszkańców. Największe zagrożenia dla bezpieczeństwa wynikają z: terroryzmu, międzynarodowego nielegalnego obrotu środkami odurzającymi czy prania brudnych pieniędzy, oszustwa zorganizowanego, fałszowania euro oraz handlu ludźmi; <https://www.europol.europa.eu>, 28 marca 2023 r.

[3] Europol, Economic Crime, <https://www.europol.europa.eu/crime-areas/economic-crime>, 19 października 2023 r.

[4] Światowe Forum Ekonomiczne (ang. *World Economic Forum*, WEF) — szwajcarska fundacja non-profit znana z organizacji corocznej konferencji w Davos, <https://pl.wikipedia.org/wiki/%C5%9Awiatowe_Forum_Ekonomiczne>, 28 marca 2023 r.

stępczości Ekonomicznej Komendy Głównej Policji, wydziały zwalczania przestępczości ekonomicznej Centralnego Biura Śledczego Policji oraz Departament Zwalczania Przestępczości Ekonomicznej Krajowej Administracji Skarbowej.

W obecnych czasach przestępstwa finansowe, popełniane w cyberprzestrzeni, zawsze popełniane są zarówno z wykorzystaniem narzędzi hackerskich, jak i wszelkiego rodzaju narzędzi wykorzystujących metody socjotechniczne. Omijają wszelkie możliwe zabezpieczenia, m.in. zabezpieczenia rządowych instytucji finansowych oraz różnego rodzaju instytucji korporacyjnych[5]. Takie postępowanie prowadzi do postrzegania różnego rodzaju przestępstw finansowych w niejednakowym świetle. Zatarły się różnice między przestępstwami finansowymi, hakowaniem czy socjotechniką wykorzystywaną dla osiągnięcia korzyści ekonomiczno-finansowych.

Postęp technologiczny, umiejętności techniczne czy szeroko pojęta praktyka dostępne są zarówno dla przestępców, jak i organów ścigania. Dla tych ostatnich niestety istnieją duże ograniczenia finansowe, które doprowadzają do braku możliwości eliminacji zorganizowanych grup przestępczych. Zrozumienie taktyki popełniania przestępstw oraz metod i technik ich zwalczania staje się z dnia na dzień coraz trudniejsze.

Wielu autorów literatury fachowej, opisujących branżę zwalczania cyberprzestępczości, określa ją jako wyzwanie XXI w., ponieważ jest zgodna z postępującą cyfryzacją, zmianami finansowymi oraz eksplozją i ekspansją popularności kryptowalut. Taka symbioza przestępstw finansowych czy gwarancji cyberbezpieczeństwa sprawia, że instytucje finansowe wykorzystują opracowane przez siebie metody ochrony swoich aktywów przy wykorzystaniu narzędzi analitycznych funkcjonujących w czasie rzeczywistym, gwarantujących przechwytywanie np. ataków sieciowych, a tym samym zapobiegają stratom finansowym. Istnieją jednak modele zabezpieczeń, które wykazują brak zdolności do zapobiegania takim atakom oraz algorytmom radzenia sobie z takimi atakami[6]. Analitycy zalecają opracowanie i wdrożenie najnowszych metod w różnych organizacjach, które zapobiegają dalszym stratom biznesowym, utracie danych osobowych klientów oraz reputacji firmy. Nowe metody wdrażane w środowisku naukowym i przemyśle to uczenie maszynowe i modele uczenia głębokiego.

Aby zwalczać cyberprzestępczość ekonomiczną, należy zwrócić szczególną uwagę na wykrywanie anomalii (*Anomaly Detection*; dalej jako: AD), które jest jedną z metod identyfikowania przestępców finansowych w sieci lub umożliwia wykrycie czy zapobieżenie występowaniu nielegalnych transakcji finansowych. Wraz ze wzrostem możliwości technicznych oraz pomysłowością cyberprzestępców, a także ewoluującymi narzędziami służącymi do maskowania tożsamości ochrona zarówno zasobów publicznych, jak i prywatnych staje się coraz trudniejsza. Wykrywanie anomalii grupowych (*Group Anomaly Detection*; dalej jako: GAD) to kolejny etap wykrywania anomalii, jakie generuje przestępca wykorzystujący wiele fałszywych tożsamości lub jakie generuje on poprzez współpracę ze zorganizowaną grupą przestępczą.

[5] S. Hasham, S. Joshi, D. Mikkelsen, *Financial Crime and Fraud in the Age of Cybersecurity*, Shanghai 2019.

[6] *Fighting Financial Crime With AI*, <https://www.ibm.com/downloads/cas/WKLQKD3W>, 29 marca 2023 r.

Tło (*Background*)

Próba przedstawienia zwalczania cyberprzestępczości ekonomicznej przy wykorzystaniu sztucznej inteligencji (AI) niesie ze sobą konieczność przedstawienia anomalii jako środka do wykrywania przestępczości ekonomicznej w cyberprzestrzeni. Istnieje także konieczność krótkiego scharakteryzowania metod wykrywania anomalii oraz metod głębokiego uczenia, które są wykorzystywane do zwrócenia uwagi organów ścigania w kierunku ujawnienia działalności przestępczej.

Typy anomalii

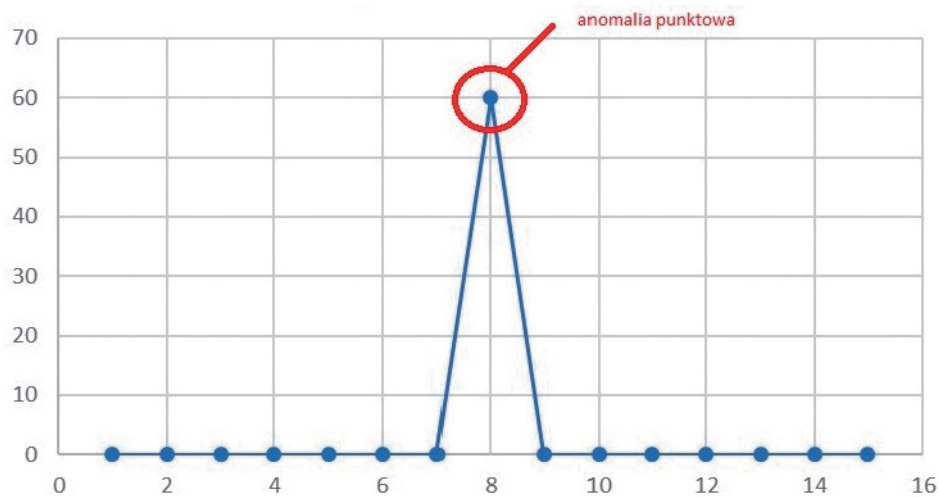
Anomalia to nic innego jak coś bardzo rzadkiego, dziwnego, odbiegającego od określonej normy, często nienaturalnego. W nauce anomalia to odchylenie od średniej lub obserwacja odbiegająca od innych obserwacji[7]. Anomalie dzielimy na: punktową, kontekstową, zbiorową.

Anomalia punktowa

Anomalia punktowa *(Point Anomaly)* to nic innego jak punkt w strumieniu danych, który odstaje od jej reszty, często nazywany odstającym[8]. Rysunek 1 ilustruje anomalię punktową.

Rysunek 1

Seria danych z anomalią punktową



Źródło: opracowanie własne

[7] A.A. Cook, G. Misirli, Z. Fan, *Anomaly Detection for IoT Time-Series Data: A Survey*, "IEEE Internet Things Journal" 2020, No. 7, s. 6481–6494.

[8] C.C. Aggarwal, *Outlier analysis in Data Mining*, Cham 2015, s. 237–263.

Anomalia kontekstowa

Anomalia kontekstowa *(Contextual Anomaly)* to punkt, który jest normalny w pewnym określonym momencie, ale nieprawidłowy w innym. Taka anomalia wymaga znajomości kontekstu, czyli normalnego zachowania. Nazywana jest również anomalią warunkową[9]. Ten typ anomalii jest powszechny w strumieniach danych generowanych dla szeregów czasowych. Na przykład duży ruch na „kołowrotku" czy szlabanie dla samochodów, które wjeżdżają na teren ogrodzonej posesji jest normalny przed godziną rozpoczęcia pracy czy po godzinie jej zakończenia, ale np. w połowie dnia pracy jest kontekstowo anomalnym zachowaniem. Taka sytuacja może powstać w wyniku np. pożaru czy katastrofy budowlanej. W przypadku tego typu anomalii musimy analizować również inne zależne parametry które umożliwią nam uznanie odchylenia od średniej za anomalię czy zakwalifikowanie do typowego zachowania. Rysunek 2 przedstawia przykład anomalii kontekstowej.

Rysunek 2

Seria danych z anomalią kontekstową

Źródło: opracowanie własne

Anomalia zbiorowa

Anomalię zbiorową *(Collective Anomaly)* można wykryć poprzez analizę strumienia danych w celu poznania jego zbiorowego normalnego zachowania. Każde odchylenie od normalnego wzorca może prowadzić do zbiorczej anomalii w odniesieniu do całych wzorców danych następujących

[9] X. Song i in., *Conditional anomaly detection*, "IEEE Transactions on Knowledge and Data Engineering" 2007, Vol. 19, No. 5, s. 631–645.

w kolejnych określonych przedziałach czasowych. Na przykład pojedyncza obserwacja w odstępie czasu nie jest wystarczająca do określenia zachowania serca[10], podczas gdy zbiorcze sygnały mogą determinować prawidłowe lub nieprawidłowe zachowanie — jak pokazano na rysunku 3. Widać tutaj, że wzorzec obserwacji jest anomalny we wskazanym przez czerwoną elipsę trzecim piku rytmu serca, dokładnie w czasie odpoczynku — wydłużony czas, w porównaniu z resztą zarejestrowanych sygnałów (ciągu danych). Wszelkiego rodzaju anomalie zbiorowe są związane z jednostką czasu, natomiast możliwe jest występowanie trendów sezonowych w takich strumieniach danych[11]. Na przykład sygnał tętna może być nieprawidłowy z powodu odczytu zaraz po biegu lub aktywności fizycznej. Podobnie sprzedaż lodów wzrasta w okresie letnim i spada pod koniec sezonu letniego. Efekt sezonowości możemy zaobserwować również w zużyciu ilości gazu ziemnego, które wzrasta zimą a maleje latem.

Rysunek 3

Seria danych z anomalią zbiorową

Źródło: <https://kredos.pl/artykuly/kardiologia/rodzaje-arytmii-oraz-obraz-ekg>, 19 października 2023 r.

Wykrywanie anomalii

Detekcja anomalii polega na wykorzystaniu myślenia komputacyjnego[12] (obliczeniowego) oraz technik matematycznych (obliczeniowych), dzięki czemu możliwe stanie się wykrycie punktów nieprawidłowych (anomalii) w zbiorze danych. Literatura przedmiotu nazywa detekcję anomalii jako detekcja ostańców, detekcja nowości, detekcja szumu czy detekcja odchyleń, a definiuje jako proces analizy zbioru danych w celu identyfikacji przypadków dewiacji. Obejmuje on:

— identyfikację nieprawidłowych danych, np. szumów, odchyleń lub wartości odstających od oryginalnego zbioru danych,

[10] M. Ahmed, A.N. Mahmood, M.R. Islam, *A survey of anomaly detection techniques in financial domain*, "Future Generation Computer Systems" 2016, Vol. 55, s. 278–288.

[11] A.V. Metcalfe, P.S. Cowpertwait, *Introductory Time Series With R*, New York 2009.

[12] A. Męczkowska-Christiansen, J. Charuta-Kojkoł, J. Zacniewska, *Computational thinking on the background of the theory of mind and didactic strategies of its development,* „Colloquium" 2021, t. 13, nr 4.

— odkrywanie nowych instancji danych na podstawie pozyskanej wiedzy o postaci oryginalnego zbioru danych.

Wykrywanie anomalii możemy wykorzystywać do:

— wykrywania oszustw,
— analizy jakości danych,
— skanowania poziomów bezpieczeństwa,
— monitorowania stanu procesów oraz systemów,
— monitorowania obrazów statycznych oraz sekwencji wideo,
— wykrywania spamu,
— wykrywania złośliwych ataków,
— oczyszczania danych przed trenowaniem modeli statystycznych czy sieci neuronowych,
— analizy zachowań ludzkich,
— wykrywania błędów czujników[13].

Wykrywanie anomalii grupowych

Wykrywanie anomalii grupowych to technika służąca do identyfikacji zbiorów lub klastrów punktów danych, które są nienormalne lub niespójne ze wzorcem grupy[14]. Podobnie jak tradycyjne wykrywanie anomalii, GAD odnosi się do problemu znajdowania w grupach danych wzorców, które nie są zgodne z oczekiwanymi przez nas zachowaniami. Anomalie grupowe mogą składać się z pojedynczych anomalnych punktów, które są stosunkowo łatwe do wykrycia, powstających wokół normalnej grupy oraz anomalnych grup powstałych wokół względnie normalnych punktów, których zachowanie jako grupy jest nietypowe, znacznie trudniejsze do wykrycia jakimikolwiek metodami. Idea wykrywania anomalii grupowych[15] podzielona została na sytuacje dynamiczne i statyczne. Statyczny GAD identyfikuje takie grupy, które są sprzeczne z normalnym zachowaniem grupy, natomiast dynamiczny GAD bada różnice w stanie grupy w pewnym okresie czasu.

Metody grupowego wykrywania anomalii oparte o sieci lub grafy

Sieci lub grafy odgrywają ważną rolę w GAD, a w szczególności przy próbie ich wykrywania w związku z przestępstwami popełnianymi przy wykorzystaniu cyberprzestrzeni. Najnowocześniejsze badania oraz opublikowane algorytmy obejmują etap wstępnego przetwarzania lub bezpośrednią analizę struktur grafu czy sieci w celu identyfikacji anomalnych klastrów lub grup społecznych. Ze względu na różnorodność i mieszankę różnych rodzajów sieci i grafów dostępnych w rzeczywistych przeszukiwanych

[13] H. Darvishi i in., *Sensor-fault detection, isolation and accommodation for digital twins via modular data-driven architecture*, "IEEE Sensors Journal" 2021, Vol. 21, No. 4, s. 4827–4838.

[14] E. Toth, S. Chawla, *Group deviation detection methods: A survey*, "ACM Computing Surveys" 2018, Vol. 51, No. 4, s. 1–38.

[15] Tamże.

modelach kluczowe jest wykorzystanie właściwości specyficznych dla danej aplikacji do zdefiniowania anomalii, jakie mogą wystąpić w sieciach lub grafach. Wartości odstające w sieciach możemy zdefiniować jako węzły, krawędzie, podgrafy lub podgrupy. Grafy czasoprzestrzenne mają dokładnie takie same wartości anomalne, z wyjątkiem ewoluującego i dynamicznego charakteru, co generuje dodatkowe trudności w identyfikacji tych wartości. Metody oparte na sieciach czy węzłach pozwalają na wykrycie anomalii grupowych w Big Data, sieciach społecznościowych, sieciach bankowych, związkach chemicznych czy w grafach wiedzy, takich jak sieć cytowań, sieć bibliografii i wielu innych dziedzinach życia lub nauki.

Głębokie uczenie

Głębokie uczenie (*Deep Learning*; dalej jako: DL) to poddziedzina uczenia maszynowego (*Machine Learning*; dalej jako: ML), która wykorzystuje sztuczne sieci neuronowe do uczenia się reprezentacji lub cech zbioru danych wejściowych. Podobnie jak w przypadku grafów, DL odgrywa kluczową rolę w przyszłości AD i GAD. Zaletą stosowania modeli głębokiego uczenia jest to, że sieci neuronowe mogą uczyć się własnych połączeń z określonymi punktami danych poprzez metodę wstecznej propagacji. Dzięki temu poszczególne dane wejściowe są ważone w różny sposób w całym zbiorze danych wejściowych. Pozwala to na ominięcie konieczności ręcznego wykrywania cech anomalnych[16]. Jednak metoda wstecznej propagacji zazwyczaj wykorzystuje metody zstępowania gradientowego jako formę funkcji straty, a to może spowodować, że minimalizacja straty nie osiągnie optymalnego punktu ze względu na to, że powierzchnia funkcji straty ma wiele lokalnych minimów, a globalne minimum może nie zostać odkryte. Rodzaje modeli DL to autoenkodery, rekurencyjne sieci neuronowe (*Recurrent Neural Networks*; dalej jako: RNN) i grafowe sieci neuronowe (*Graph Neural Networks*; dalej jako: GNN). Istnieją modele hybrydowe będące mieszanką DL i ML[17] wykorzystujące sieć DBN (*Deep Belief Network*) wytrenowaną do wyodrębnienia cech zasadniczych, a następnie wykorzystano wytrenowanie jednoklasowej maszyny wektorów nośnych (*Support Vector Machin*, SVM) na cechach wyuczonych przez model DBN.

Rodzaje nadzoru wykrywania anomalii skupiają się na prawdach podstawowych i zdolności wykorzystywanych modeli do poprawnego klasyfikowania anomalii za pomocą posiadanych informacji. Rodzaje te to:

— nadzorowane wykrywanie anomalii — modele wymagają dostępności do etykiet dla definicji normalności i nienormalności,
— półnadzorowane wykrywanie anomalii — jako dane wejściowe wykorzystywane są tylko normalne próbki danych lub tylko nienormalne

[16] R. Chalapathy, S. Chawla, *Deep learning for anomaly detection: A survey*, s. 1–50, 2019, <https://www.researchgate.net/publication/330357393_Deep_Learning_for_Anomaly_Detection_A_Survey>, 19 października 2023 r.

[17] S.M. Erfani i in., *Highdimensional and large-scale anomaly detection using a linear one-class SVM with deep learning*, "Pattern Recognition" 2016, Vol. 58, s. 121–134.

próbki danych; algorytm próbuje modelować pojedynczą koncepcję i wykrywa anomalię w zależności od kondycji danych wykorzystywanych w budowaniu koncepcji,
— wykrywanie anomalii bez nadzoru — stosowane w sytuacji, gdy nie jest znana wcześniejsza wiedza o zbiorze danych oraz nie są znane informacje o etykietach,
— *Human-in-the-loop* — aktywne uczenie odpowiada konfiguracji, w której algorytm uczenia może selektywnie odpytywać człowieka — analityka o etykiety instancji wejściowych, aby poprawić swoją dokładność predykcji.

W chwili obecnej AD ukierunkowuje się w stronę jednoczesnego wykorzystania modeli grafowych i algorytmów głębokiego uczenia i nazwano je GNN. Przykłady GNN to np. *Recurrent Graph Neural Networks*, *Graph Convolutional Networks* czy *Spatio-Temporal Graph Neural Networks*[18].

Aktorzy i ofiary

W języku UML[19] Aktor to użytkownik lub zewnętrzny system, z którym modelowany system wchodzi w interakcje[20]. W tym opracowaniu użyjemy słowa aktor — w znaczeniu cyberprzestępca. Aby zrozumieć anomalne zachowania generowane przez aktorów, musimy pogłębić wiedzę na temat ich typowych działań poprzez badanie wzorców społecznych i ich cech psychologicznych. Aktorzy nieustannie dostosowują swoje metody działania, aby utrzymać swoją silną pozycję w wytworzonym przez siebie ekosystemie.

Aktorzy i ich typowe działania

Zaufanie

Psychologowie społeczni i neuronaukowcy opisują zaufanie jako skuteczny mechanizm wykorzystywany przez ludzi do radzenia sobie ze złożonością, zwłaszcza w sytuacjach ryzyka i niepewności. Niewiele jest obszarów współczesnej cywilizacji, które są większą wylęgarnią niepewności niż podziemie związane z cyberprzestępczością. Trzeba mieć świadomość, że aktorzy rzadko dopuszczają się przestępstw wobec osob, które znają w prawdziwym życiu. Skuteczni aktorzy doskonale zdają sobie sprawę z tego, jak ważne jest zaufanie, rozumiejąc, że muszą przekazywać elementy znajomości, podobieństwa i wiedzy technicznej, aby zachęcać do „udanych" zachowań, jakie założyli na początku swojej działalności.

[18] Z. Wu i in., *A comprehensive survey on graph neural networks*, "IEEE Transactions on Neural Networks and Learning Systems 2021, Vol. 32, No. 1, s. 4–24.

[19] *Unified Modeling Language* (zunifikowany język modelowania, UML) — język półformalny wykorzystywany do modelowania różnego rodzaju systemów, stworzony przez Grady'ego Boocha, Jamesa Rumbaugha oraz Ivara Jacobsona, obecnie rozwijany przez Object Management Group, <https://pl.wikipedia.org/wiki/Unified_Modeling_Language>, 19 kwietnia 2023 r.

[20] S.S. Alhir, *UML. Wprowadzenie*, Gliwice 2004.

Należy mieć na uwadze fakt, że — w przypadku kiedy aktor utraci zaufanie — szybko usuwa się z danej operacji.

Świecenie przykładem

Doświadczeni aktorzy, którzy odnieśli sukces, wykazują niezwykłe zdolności w dokonywaniu skutecznych osądów i podejmowaniu decyzji. Często odzwierciedlają skuteczne, uzasadnione cechy przywódcze — są skutecznymi menedżerami, decydentami i rozwiązują problemy, ponieważ przestrzegają surowych zasad rządzących nimi i ich zespołami. Demonstrują również autorytet, delegując zadania, jednocześnie zarządzając oczekiwaniami swojego zespołu i przyciągając zdolnych, zmotywowanych finansowo i wysoko wykwalifikowanych partnerów. Aktorzy ci często przebijają się przez szum wśród swoich rówieśników i media, koncentrując się przede wszystkim na osiąganych zyskach finansowych.

Dostosuj się lub giń

Kiedy wystąpią zakłócenia w działalności aktora — takie jak załatanie luk w zabezpieczeniach, wyciek kodu źródłowego lub zakłócenie infrastruktury — sposób, w jaki radzi on sobie z tymi zmianami, może zadecydować o jego długoterminowym sukcesie lub go zniweczyć. Zaobserwowano, że grupy cyberprzestępcze, które osiągają wysokie wyniki, wielokrotnie opracowują nowe złośliwe oprogramowanie oraz restrukturyzują zespoły i operacje dynamicznie do pojawiających się nowych potrzeb. Najskuteczniejsi aktorzy często są najpierw rozpoznawani w mediach lub przez elitarnych badaczy, którzy są pionierami pewnych metod ataku, zanim inni szybko skopiują ich działania. Niezależnie od tego, czy są dobrzy w samodzielnym myśleniu, zastanawianiu się nad przyszłością czy przestawianiu się na alternatywne plany, ci aktorzy wiedzą, że zmiana jest stała i konieczna, a takie zachowania gwarantują coraz większą rentowność.

Bez twarzy

Skuteczni aktorzy wykorzystują wszystkie możliwe warstwy anonimowości, które dostarcza Internet w celu ukrycia prawdziwej tożsamości. Większa anonimowość gwarantuje większe bezpieczeństwo. Trudność zidentyfikowania aktora zwiększa szanse, że nie zostanie on złapany i osądzony. Jednak ci aktorzy, którzy chcą odnieść sukces, muszą osiągnąć odpowiednią równowagę między byciem wystarczająco znanym, dzięki czemu zyskują wiarygodność, a ukrytym. Ci z podziemia, którzy to zrównoważyli, zazwyczaj wdrażają lepsze praktyki zwiększające bezpieczeństwo (OPSEC[21]), takie jak używanie adresów e-mail i kont niezwiązanych z kontami osobistymi, aby w żadnej formie nie być powiązanym z prawdziwą

[21] OPSEC to proces ochrony poszczególnych fragmentów danych, które można zgrupować, aby uzyskać większy obraz, <https://en.wikipedia.org/wiki/Operations_security>, 19 kwietnia 2023 r.

tożsamością. Starają się również unikać ujawniania danych osobowych podczas rozmów na forach, czatach czy w mediach społecznościowych.

Aktorzy wykorzystują różnorodne narzędzia, takie jak usługi *bulletproof hosting*[22] (BPH), przeglądarki Tor[23] i sieci VPN[24], aby chronić swoją infrastrukturę i tożsamość. Aktorzy również anonimizują swoje fundusze i transakcje dzięki usługom mieszania kryptowalut. Próbują sprawić, by fundusze i transakcje kryptowalutowe były niewykrywalne, przez co zyski aktora będą rzadziej śledzone przez organy ścigania.

Takie strategie i narzędzia nie zawsze wystarczają, aby umożliwić aktorom zachowanie anonimowości. Odnoszący sukcesy cyberprzestępcy monitorują, ile uwagi poświęcają sobie i wiedzą, kiedy się ukryć. Zazwyczaj wracają z nowym aliasem i ulepszoną strategią działania, co gwarantuje im pozostanie bezpiecznymi. Jeśli nie powrócą, znaczy, że zaczynają korzystać z „zarobionych" funduszy.

Łatwo to zrobić

Aktorzy na wszystkich poziomach umiejętności wybierają najłatwiejszą możliwą ścieżkę do zarobienia pieniędzy. Skuteczni angażują się w aktywne skanowanie — proces, który jest niezwykle łatwy do skonfigurowania i zautomatyzowania — w celu skutecznego atakowania organizacji poprzez wykorzystywanie podmiotów z niezałatanymi lukami w zabezpieczeniach. Następnie towarzyszą temu ataki typu *brute-force* i wypychanie danych uwierzytelniających na systemy podrzędne w celu uzyskania dostępu do sieci. Taki proces jest podstawą działania wielu aktorów, którzy są znani jako najlepsi brokerzy dostępu do sieci w podziemiu cyberprzestępczym. Ich strategia biznesowa polega na sprzedawaniu dużych ilości dostępu globalnym organizacjom z różnych sektorów, aby przyciągnąć wielu nabywców. Ta taktyka została przyjęta przez wielu innych aktorów, którzy wydają się atakować każdą organizację, do której mogą łatwo uzyskać początkowy dostęp, zamiast poświęcać czas i wysiłek na atakowanie konkretnych organizacji. Niektórzy z odnoszących największe sukcesy aktorów stosowali te strategie i zlecali na zewnątrz sposoby uzyskiwania dostępu, posuwając się nawet do zatrudniania testerów penetracyjnych w celu uzyskania dostępu do własnych programów.

Wiedza to potęga

Aktorzy cyberprzestępczy, którzy osiągają wysokie wyniki, często są dociekliwi i uczą się przez całe życie. Są biegli w technologii, szukają mentorów, zapisują się na legalne i nielegalne kursy, śledzą media techniczne, uczęszczają na wykłady i odkrywają nowe obszary naukowo-badawcze. Kursy szkoleniowe, przewodniki krok po kroku, podręczniki i prezentacje wideo

[22] <https://us.norton.com/blog/emerging-threats/what-is-bulletproof-hosting#>, 19 kwietnia 2023 r.

[23] <https://pl.wikipedia.org/wiki/Tor_(sieć_anonimowa)>, 19 kwietnia 2023 r.

[24] <https://pl.wikipedia.org/wiki/Wirtualna_sieć_prywatna>, 19 kwietnia 2023 r.

umożliwiają aktorom podniesienie poziomu umiejętności lub wyrafinowania. Niezależnie od tego, czy jest to czysto techniczne, czy zakorzenione w inżynierii społecznej, ciągłe dążenie do wiedzy pomaga skutecznie osiągać swoje cele.

Przestępczość zorganizowana

Z biegiem czasu sieci cyberprzestępcze stały się bardziej zorganizowane, współpracujące i dobrze finansowane. Wysoko wykwalifikowani aktorzy rozwijają swoje działalności i ponownie inwestują część zarobków w swoje przedsięwzięcia. Podobnie jak w przypadku innych profesjonalnych przedsięwzięć biznesowych, cyberprzestępcy reinwestują zyski z powrotem w nielegalne przedsięwzięcie, aby poprawić swoje możliwości, infrastrukturę, platformy i oferty. Poszerza to ich możliwości doskonalenia umiejętności technicznych i umożliwia przeprowadzanie bardziej wyrafinowanych ataków. W ciągu ostatniej dekady nastąpiła wyraźna zmiana w sposobie, w jaki aktorzy traktują swoje działania. Ogólnie rzecz biorąc, grupy cyberprzestępców postrzegają negocjacje i metodologie ataków z nastawieniem biznesowym, szczególnie w odniesieniu do profesjonalizacji swoich usług i sposobu, w jaki się komunikują. Zamiast reagować emocjonalnie, podchodzą do interakcji ze standardowymi procedurami operacyjnymi i wyjaśniają oczekiwania partnerów na wczesnym etapie i często w trakcie trwania relacji.

Ofiary

Wszyscy jesteśmy ludźmi z własnymi unikalnymi dziwactwami, wadami i zachowaniami, co zauważają i wykorzystują aktorzy. Wraz z nieustannym rozwojem i transformacją technologii mają oni do dyspozycji kilka rodzajów działań, które mogą wykorzystać na swoją korzyść. Wykorzystują nasze identyfikatory, tendencje i skłonności, aby uzyskać dostęp do rzeczy, które cenimy najbardziej i o których bezpieczeństwo dbamy.

Oto niektóre z najczęstszych ludzkich zachowań wykorzystywanych przez aktorów do przeprowadzania wszelkiego rodzaju złośliwych ataków czy popełniania czynów zabronionych.

Ciekawość

Ludzie mają naturalną skłonność do eksploracji i rozwiązywania zagadek. Wykorzystują to oszuści phishingowi, wysyłając złośliwe linki, które przenoszą niczego niepodejrzewającego użytkownika do spreparowanych stron internetowych lub umożliwiają im pobranie niebezpiecznego oprogramowania.

Wiarygodność

Ludzie zazwyczaj ufają witrynom i wiadomościom e-mail, które wyglądają znajomo i autentycznie, więc oszuści ukrywają swoje witryny przed

niczego niepodejrzewającymi użytkownikami pod pozorem witryny rządowej lub korporacyjnej.

Luźne nawyki bezpieczeństwa

Większość ludzi ma tendencję do używania tych samych haseł lub używania haseł słabych, co ułatwia cyberprzestępcom ich odgadnięcie i uzyskanie dostępu do kont oraz przejęcie poufnych informacji.

Dbałość o szczegóły

Osoby często pomijają szczegóły i nie czytają drobnego druku w formularzach internetowych. Cyberprzestępcy wiedzą o tym i wykorzystują to, ponadto sami uzupełniają brakujące informacje, aby uzyskać dostęp do kont i danych użytkowników.

Brak świadomości

Ludziom często brakuje świadomości cyberbezpieczeństwa i łatwo dają się oszukać pozornie godnym zaufania podmiotom cyfrowym, takim jak strony internetowe i e-maile. Ten brak czujności wykorzystują cyberprzestępcy do uruchamiania złośliwego oprogramowania i uzyskiwania dostępu do danych osobowych.

Cyberprzestępczość finansowa

Cybernetyka zapewnia przestępcom wiele możliwości — atakowanie pojedynczych komputerów, sieci, infrastruktury krytycznej, przetrzymywanie pieniędzy czy danych dla wymuszenia okupu. Ułatwia popełnianie przestępstw, oszustw na dużą skalę, globalnie wpływa na poziom bezpieczeństwa narodowego. Dziś już wiadomo, że ryzyko cybernetyczne to w rzeczywistości ryzyko biznesowe, a bezpieczeństwo cybernetyczne to bezpieczeństwo narodowe. W 2022 r. do Centrum Skarg o Przestępstwach Internetowych FBI[25] (IC3) wpłynęły 800 944 skargi o całkowitej stracie finansowej ponad 10,2 miliarda dolarów. Raport FBI wyszczególnił także liczbę skarg i ofiar, szeroką gamę wykorzystywanych typów przestępstw oraz zgłoszone kwoty pieniędzy zarówno skradzionych przez przestępców, jak i następnie odzyskanych przez zespół FBI *Recovery Assets Team* (RAT). W tabeli 1 przedstawiono liczbę ofiar dla wybranych typów przestępstw zgłoszonych w Stanach Zjednoczonych w 2022 r., oraz skradzione przy wykorzystaniu tej metody kwoty (łącznie typów przestępstw zgłoszono 27). Największa wartość działalności przestępczej pochodzi podobno z inwestycji na kwotę łącznie ponad 3,3 miliarda dolarów. Raport

[25] FBI, *Internet Crime Report 2022*, <https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf>, 19 kwietnia 2023 r.

ten podkreśla ogromne kwoty, które można wyłudzić od ofiar cyberprzestępczości finansowej.

Tabela 1

Liczba ofiar dla wybranych typów przestępstw zgłoszonych w Stanach Zjednoczonych w 2022 r. oraz kwoty skradzione przy wykorzystaniu tej metody

Typ przestępstwa	Liczba ofiar	Stracone środki w dolarach amerykańskich
Phishing	300 497	52 mln
Pozyskanie danych osobowych	58 859	742 mln
Brak płatności/brak dostawy	51 679	281 mln
Wymuszenie finansowe	39 416	54 mln
Wsparcie techniczne	32 538	806 mln
Inwestycje	30 529	3 311 mln
Kradzież tożsamości	27 922	189 mln
Karty kredytowe/czeki	22 985	264 mln
BEC/EAC	21 832	2 742 mln

Źródło: opracowanie własne na podstawie raportu FBI (zob. przypis 25)

Sprawcy cyberprzestępstw finansowych są trudni do zidentyfikowania. Celowo maskują swoją działalność, aby wtopić swoje poczynania w normalne zachowanie każdego innego klienta lub użytkownika strony internetowej lub serwisu finansowego, jednak w przypadku zgrupowania działalności bardziej widać jej nienormalność. Grupowe wykrywanie anomalii jest metodą, która może zidentyfikować nieuregulowane wzorce zachowań aktorów, a w przypadkach zwalczania cyberprzestępczości finansowej jest bardziej dokładna niż wykrywanie anomalii punktowych.

Oszustwa inwestycyjne

Papiery wartościowe (akcje, prawa poboru, prawa do akcji, warranty subskrypcyjne, kwity depozytowe, obligacje, listy zastawne, certyfikaty inwestycyjne, inne zbywalne papiery wartościowe, inne zbywalne prawa majątkowe) pozwalają ludziom inwestować swoje pieniądze z myślą o uzyskaniu zysku na podstawie przeprowadzonych badań lub po prostu przeczucia. Wiadomo jednak, że część uczestników rynku oszukuje i dzięki temu osiąga ogromne zyski kosztem inwestorów instytucjonalnych i detalicznych, a tym samym ci drudzy ponoszą straty. Złapanie takich nieuczciwych podmiotów nie jest łatwe i zazwyczaj wymaga zaangażowania dużej liczby pracowników, którzy zmuszeni są do gromadzenia dowodów popełnianych oszustw przez długi czas. Jednak osiągnięcia ostatnich lat w zakresie aplikacji i technik uczenia maszynowego pomagają w identyfikacji

aktorów w bardziej efektywny i szybszy sposób. Niektóre z metod wykorzystywanych przez osoby dopuszczające się nieuczciwej działalności inwestycyjnej obejmują manipulację, wykorzystywanie informacji poufnych, pranie brudnych pieniędzy czy terroryzm.

Manipulacja to nic innego jak czynność polegająca na sprzedaży lub zakupie zabezpieczenia finansowego w celu celowego manipulowania ceną bazowego składnika aktywów lub zabezpieczenia. Nielegalny *insider trading* czy *insider dealing* ma miejsce, gdy „insiderzy", czyli osoby mające dostęp do prywatnych i niepublicznych materiałów spółki, wykorzystują te informacje przed ich publicznym rozpowszechnieniem w celu osiągnięcia korzyści pieniężnych. Obejmuje to nie tylko obrót papierami wartościowymi, ale również ujawnianie informacji niepublicznych osobom trzecim.

W zakresie uczenia maszynowego i głębokiego uczenia poczyniono postępy w odniesieniu do rozwiązania tych dwóch obszarów. Opracowane w ostatnich latach metody trenowania i wykorzystania sieci neuronowych mogą pomóc w wykrywaniu grup osób mających dostęp do informacji poufnych lub współkonspiratorów w odniesieniu do *insider tradingu*. Algorytmy te są także w stanie zidentyfikować potencjalne manipulacje rynkowe poprzez analizę portfela zamówień akcji w celu odkrycia powiązań handlowców lub brokerów działających w nietypowy sposób (anomalny), który byłby sprzeczny z korzyściami ich klientów lub szerszego rynku inwestorów.

Jeden z algorytmów to system uczenia zespołowego oparty na RNN do wykrywania manipulacji kursami akcji. Zbiór treningowy został zbudowany z przypadków pobranych z *China Securities Regulatory Commission* wraz z odpowiadającymi im danymi finansowymi. Dalszy etap rozwoju zaproponowanego algorytmu to wykorzystanie metod analizy szeregów czasowych danych dotyczących obrotu giełdowego przy wykorzystaniu LSTM[26]. Zastosowanie LSTM daje także możliwość analizy relacji społecznych kadry kierowniczej firmy oraz treści ogłoszeń, dzięki czemu znacznej poprawie ulegnie możliwość wykrywania manipulacji z jednoczesną możliwością identyfikacji *insider tradingu*[27].

Pranie brudnych pieniędzy

Metoda stosowana przez przestępców lub osoby posiadające „brudne" (nielegalne) środki finansowe uzyskane najczęściej w wyniku działalności przestępczej mająca na celu wprowadzenia ich do legalnego obrotu gospodarczego. Koronna Służba Prokuratorska (*Crown Prosecution Service* — CPS) w Wielkiej Brytanii[28] definiuje schemat prania pieniędzy jako obejmujący zazwyczaj trzy etapy. Pierwszym etapem jest lokowanie brudnych pieniędzy, czyli proces deponowania pieniędzy pochodzących

[26] Pamięć krótkotrwała i długotrwała — *Long short-term memory*, LSTM — rodzaj RNN.

[27] Q. Wang i in., *Enhancing intraday stock price manipulation detection by leveraging recurrent neural networks with ensemble learning*, "Neurocomputing" 2019, Vol. 347, s. 46–58, <https://doi.org/10.1016/j.neucom.2019.03.006>, 19 kwietnia 2023 r.

[28] *Money Laundering Offences*, <https://www.legislation.gov.uk/ukpga/2002/29/part/7>, 19 kwietnia 2023 r.

z przestępstwa w jakimś systemie finansowym. Drugim etapem jest warstwowanie, czyli przemieszczanie pieniędzy w ramach systemu finansowego poprzez skomplikowane sieci transakcji w celu ich ukrycia. Warstwa ta jest zwykle realizowana za pośrednictwem spółek *offshore*. Wreszcie trzeci etap obejmuje integrację, która polega na wchłonięciu lub wtopieniu pieniędzy pochodzących z przestępstwa w realną gospodarkę poprzez takie inwestycje jak nieruchomości, zakup akcji czy luksusowych przedmiotów.

Uczenie maszynowe i uczenie głębokie zyskały na popularności w walce z praniem brudnych pieniędzy i próbą identyfikacji nielegalnych transakcji przy wykorzystaniu internetowych sieci społecznościowych i kryptowalut. O przeciwdziałaniu praniu pieniędzy z wykorzystaniem walut wirtualnych w świetle krajowych i międzynarodowych regulacji AML[29] napisał Paweł Opitek[30], natomiast jeden z dużych azjatyckich serwisów społecznościowych posiada w swojej sieci cyfrową walutę, pozwalającą użytkownikom na dokonywanie transakcji z innymi użytkownikami w celu dokonania zakupów, a także na przekazywanie cyfrowej waluty innym osobom w sieci. Jednym z problemów tego serwisu jest właśnie pranie cyfrowej waluty.

Do wykrycia kont służących do prania wykorzystano DNN[31]. Na początku wytypowano około 500 tysięcy kont i oznaczono je jako łagodne lub złośliwe, śledząc ogłoszenia o taniej wirtualnej walucie w głównych dostępnych sklepach internetowych. Następnie dokonano analizy stron internetowych, które odwiedzali właściciele tych kont oraz skojarzono logowania z adresami IP w celu dalszej identyfikacji złośliwej aktywności. Funkcje zostały zaprojektowane w taki sposób, aby identyfikować zachowania konta, takie jak: aktywność na koncie, np. wgrywanie zdjęć lub zaangażowanie na stronie poza finansami, metody doładowania cyfrowej waluty, wypłaty, wydatki i darowizny. Sekwencje aktywności finansowej były modelowane przy użyciu dyskretnego czasowego modelu łańcucha Markowa. Uchwycone sekwencje zostały wykorzystane jako cechy w modelu. Cechy te następnie ładowano do grafu, który używano jako globalny przegląd zachowań związanych z transferem waluty pomiędzy kontami. W następnej kolejności przy użyciu metody *Fast Unfolding*[32], która znajduje struktury społecznościowe w dużych sieciach, identyfikowane były podgrafy, które mapują konta złośliwe do złośliwych, łagodne do łagodnych oraz złośliwe do łagodnych. Do identyfikacji złośliwych kont w utworzonych cechach wykorzystywano klasyfikatory statystyczne. Użyto klasyfikatory SVM, *random*

[29] System zwalczania prania pieniędzy i finansowania terroryzmu. Polski system przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu (AML/CFT) kształtowany jest przede wszystkim przez regulacje prawne zarówno krajowe, jak i unijne (UE). Podstawowym aktem prawnym w tym zakresie jest ustawa z 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (tekst jedn. DzU z 2023 r., poz. 1124); AML/CFT, <https://www.gov.pl/web/finance/aml-cft>, 9 maja 2023 r.

[30] P. Opitek, *Przeciwdziałanie praniu pieniędzy z wykorzystaniem walut wirtualnych w świetle krajowych i międzynarodowych regulacji AML*, „Prokuratura i Prawo" 2020, nr 12, s. 41–70.

[31] Y. Zhou i in., *Analyzing and detecting money-laundering accounts in online social networks*, "IEEE Network" 2018, Vol. 32, No. 3, s. 115–121.

[32] V. Blondel i in., *Fast unfolding of communities in large networks*, "Journal of Statistical Mechanics: Theory and Experiment" 2008, Vol. 2008, s. 1–12.

forest i regresji logistycznej. Dały one bardzo wysokie wyniki dokładności (TP — *True Positive*) — 94,2% przy bardzo niskim współczynniku fałszywych wyników pozytywnych (FP — *Folse Positive*) — 0,97%. Metryka przyrostu informacji została wyodrębniona z cech po to, aby zidentyfikować ich znaczenie dla wyznaczonego modelu. Najlepsze cechy obejmowały procent liczby wydatków na prezenty w społeczności i normalizację liczby kont docelowych w społeczności. Pięć najlepszych wyodrębnionych cech, wszystkie z zyskiem informacyjnym > 0,5 zostały wyodrębnione z przyjętego modelu. Bez użycia metod wykrywania anomalii grupowych, takich jak *Fast Unfolding*, w celu wykrycia podgrup w ogólnej społeczności sieci społecznej, dokładność przyjętego modelu byłaby naruszona, ponieważ nie zostałyby uwzględnione cechy o najwyższym zysku informacyjnym.

Przestępcy tworzą struktury organizacyjne z myślą o obfuskacji[33]. Do walki z nimi niezbędna jest identyfikacja całych sieci, aby zrozumieć i określić role ich poszczególnych członków. Poprzez integrację algorytmów, dokonanie analizy sieci społecznych[34] oraz przy wykorzystaniu danych z kont bankowych i krajowego rejestru sądowego dochodzi do skonstruowania i analizy sieci społecznych podczas prowadzenia śledztwa dotyczącego AML. Badaczom udało się zidentyfikować kluczowe elementy pierścieni prania pieniędzy. Byli w stanie ujawnić prawdziwych liderów i ich słabe punkty. Byli również w stanie wykryć, które konta są w posiadaniu tej samej osoby. Zaimplementowane techniki klastrowania pozwoliły znaleźć i przypisać konkretne role do osób w sieci. Wynika z tego, że połączenie technik uczenia maszynowego z analizą sieci społecznych może być potężnym narzędziem w ustalaniu sieci przestępczości i przeciwdziałaniu praniu pieniędzy. Narzędzia te, w połączeniu z ludźmi w pętli, takimi jak specjaliści od egzekwowania prawa lub AML, mogą przynieść bardzo dokładne i obiecujące wyniki.

Kryptowaluty

Według CipherTrace[35], raport marzec 2023 r., straty w ramach siedmiu głównych metod dokonywania włamań, oszustw czy kradzieży kryptowalut sięgnęły 383 miliony dolarów, natomiast na koniec III kwartału łączna kapitalizacja rynkowa wszystkich aktywów kryptowalutowych, w tym stabilnych monet i tokenów, wyniosła około 1,1 biliona dolarów. Jeszcze w 2019 r. oszustwa związane z decentralizacją finansów (*Decentralized*

[33] Obfuskacja — zaciemnianie kodu. Jest to technika przekształcania programów, która zmienia składnię, ale zachowuje ich semantykę, co znacząco utrudnia ich zrozumienie. Wyróżniamy 3 typy transformacji obfuskacyjnych: transformacja wyglądu (ang. *Layout Transformation*), transformacja danych (ang. *Data Transformation*), transformacja kontroli (ang. *Control Transformation*), <https://pl.wikipedia.org/wiki/Zaciemnianie_kodu dostęp>, 9 maja 2023 r.

[34] R. Dreżewski, J. Sepielak, W. Filipkowski, *The application of social network analysis algorithms in a system supporting money laundering detection*, "Information Sciences" 2015, Vol. 295, s. 18–32.

[35] *Crypto Crimes & Anti-Money Laundering (AML) Report March 2023*, <https://ciphertrace.com/crime-and-anti-money-laundering-report-march-2023/>, 9 maja 2023 r.

Finance, *DeFi*) były rzadkością, natomiast w dzisiejszych czasach jest to około 70% całkowitej wielkości oszustw i kradzieży. Pranie pieniędzy i finansowanie terroryzmu jest możliwe właśnie dzięki wykorzystaniu kryptowaluty. Główne jednostki przestępcze działające w branży kryptowalutowej to:

— największe anglojęzyczne rynki darknetowe[36], należą do nich: AlphaBay, ASAP Market i Bohemia (AlphaBay był największym rynkiem darknetowym w 2017 r. z ponad 400 tysiącami użytkowników, zanim strona została przejęta 5 lipca 2021 r. Desnake, były administrator AlphaBay, pojawił się na forum przestępczym, aby ogłosić ponowne uruchomienie rynku. Nowy AlphaBay jest bardziej skoncentrowany na bezpieczeństwie, zwłaszcza, że rynek ten jest oparty wyłącznie na Monero[37]. W połowie września 2022 r. zgłoszone przez AlphaBay statystyki dotyczące liczby kont kupujących w witrynie przekroczyły 1 milion. Jeśli to prawda, to byłby to jeden z największych rynków tego rodzaju. AlphaBay jest obecnie największym darknetowym rynkiem Monero-only, pokonując Monopoly Market, który początkowo był serwisem Monero-only, ale ostatecznie uległ presji użytkowników i zaakceptował bitcoina).

— największe rynki darknetowe regionu Wspólnoty Niepodległych Państw (WNP), są to: OMG!OMG!, Shkaf, o3shop, Mega i BlackSprut (Obecnie konkurencja na rynkach darknetowych w regionie WNP znacznie wzrosła, głównie w Rosji. Badacze CipherTrace uważają OMG!OMG! za najbardziej znaczący obecnie działający rosyjski rynek darknetowy).

Najbardziej znaczące aktywne podmioty zajmujące się oszustwami to: Benumb, Biden Cash, Brians Club, Genesis Market, HGN01 i Rescator. Większość z nich to serwisy cardingowe[38], natomiast Genesis Market to działający od dawna rynek „botów". Strony cardingowe pomagają w kupnie i sprzedaży skradzionych informacji o kartach kredytowych. Często większe witryny cardingowe to autoshopy. Autoshop to strona cardingowa, która pozwala kupującym sprawdzić, czy skradziona karta jest nadal aktywna, a jeśli nie jest, automatycznie otrzymać zwrot pieniędzy. Boty Genesis Market odnoszą się do cyfrowych tożsamości na sprzedaż. Genesis Market sprzedaje głównie pliki cookie, cyfrowe odciski palców, skradzione dane logowania itp., aby pomóc przestępcom w podszywaniu się pod osoby i uzyskiwaniu dostępu do ich kont. Zazwyczaj na sprzedaż

[36] Dark web (net), ciemna sieć — termin określający celowo ukrytą część zasobów Internetu, którą można przeglądać jedynie przy użyciu specjalnego oprogramowania. Dostęp do Dark webu jest możliwy z poziomu tzw. sieci Darknet, składających się z wielu rozproszonych, anonimowych węzłów (np. Tor, I2P czy Freenet), <https://pl.wikipedia.org/wiki/Dark_web>, 9 maja 2023 r.

[37] Monero — kryptowaluta typu *open-source* stworzona w kwietniu 2014 r., która koncentruje się na prywatności i decentralizacji, <https://pl.wikipedia.org/wiki/Monero>, 9 maja 2023 r.

[38] Carding to termin opisujący handel i nieautoryzowane użycie kart kredytowych. Skradzione karty kredytowe lub numery kart kredytowych są wykorzystywane do kupowania przedpłaconych kart podarunkowych w celu zatarcia śladów aktorów. Działania obejmują również wykorzystywanie danych osobowych oraz techniki prania pieniędzy. Nowoczesne strony z kartami zostały opisane jako podmioty komercyjne oferujące pełen zakres usług, <https://en.wikipedia.org/wiki/Carding_(fraud)>, 9 maja 2023 r.

wystawianych jest ponad 400 tysięcy różnych tożsamości cyfrowych w jednym czasie.

Cryptocurrency mixing/tumbler to metoda stosowana przez cyberprzestępców do prania kryptowalut za pośrednictwem różnych portfeli w celu ukrycia pochodzenia środków. Odbywa się to poprzez wykorzystanie zaufanej strony trzeciej do odbierania kryptowaluty z oryginalnego adresu i wykorzystanie alternatywnego adresu do wysyłania oryginalnych środków na nowo utworzony przez użytkownika adres[39]. Jest to również wykonywane za pośrednictwem wielu adresów, aby stworzyć trudny szlak do mapowania z powrotem do oryginalnego adresu, co z kolei mogłoby zidentyfikować osobę.

Deanonimizacja blockchainów kryptowalutowych (*Deanonymizing Cryptocurrency Blockchains*, DCN)

W celu zwalczania cyberprzestępczości finansowej mającej miejsce w cyberprzestrzeni, niezbędna jest możliwość identyfikacji kontrolerów kont kryptowalutowych. W miarę jak wykorzystanie kryptowalut zaczyna rosnąć, ustawodawcy wprowadzili do prawa konieczność praktykowania AML przez niektóre giełdy kryptowalutowe. Obejmuje to wdrożenie wymogu znajomości swojego klienta (*Know Your* Customer, KYC) w całej bazie użytkowników. W dokumencie *Deanonymizing cryptocurrency with graph learning: The promises and challenges*[40] opisano podejście do deanonimizacji blochchainów bitcoinowych poprzez wykorzystanie GCN. Opisano również w nim szczegóły dotyczące cech charakterystycznych dużych sieci, które mogą posłużyć do wytrenowania DNN w celu wykrycia anomalii, czyli:

— duże i skrajnie przekrzywione wykresy,
— grafy dynamicznie rosnące,
— grafy semantyczne.

Grafy semantyczne opisują różne działania, do których blockchain może być wykorzystany, w tym np. zawieranie inteligentnych kontraktów. Dzięki GCN można:

— wykrywać adresy nieaktywny lub z zerowym saldem,
— wykrywać publicznie dostępne etykiety adresowe.

GCN jest w stanie zredukować rozmiar grafu poprzez identyfikację nieaktywnych/zerowych adresów bilansowych, co w rezultacie daje zredukowany graf dla lepszych prędkości obliczeń. Wspomniane powyżej zalety GCN, ze względu na niektóre giełdy lub strony internetowe, które mogą wymagać KYC, umożliwiają identyfikowanie tożsamości portfeli.

[39] I. Alarab, S. Prakoonwit, M. Nacer, *Competence of graph convolutional networks for anti-money laundering in bitcoin blockchain* [w:] *ICMLT '20: Proceedings of the 2020 5th International Conference on Machine Learning Technologies*, 19–21 June 2020, New York 2020, s. 23–27.

[40] A. Gaihre, S. Pandey, H. Liu, *Deanonymizing cryptocurrency with graph learning: The promises and challenges* [w:] *2019 IEEE Conference on Communications and Network Security*, Washington, 10–12 June 2019, s. 2019–2021.

Oszustwo celne

Oszustwo celne polega na uchylaniu się od zapłaty za przywóz towarów do danego kraju. Nie jest to przestępstwo popełniane wyłącznie w cyberprzestrzeni, jednak jest to przestępstwo finansowe, z którym walczy się także z wykorzystaniem uczenia maszynowego. Unijny urząd ds. zwalczania nadużyć finansowych[41] stwierdził, że oszustwa celne są finansowo szkodliwe dla legalnego przemysłu i podatnika UE. W latach 2010–2021, w ramach ponad 2400 dochodzeń w sprawie oszustw celnych, unijny urząd ds. zwalczania nadużyć finansowych odzyskał łącznie 8 miliardów euro (w 2021 r. — 212 dochodzeń na łączną kwotę 527,4 miliony euro — przy budżecie na swoją działalność 61 milionów euro). Ze względu na ogromny wolumen transakcji i ręczną kontrolę towarów wymaganą przy prowadzeniu dochodzeń w sprawie oszustw celnych nie jest możliwe, bez zaangażowania ogromnych zasobów, prześwietlenie każdego towaru importowanego do danego kraju.

Istnieją postępy w społecznościach wykorzystujących sztuczną inteligencję do badań — dążące do tego, aby stworzyć systemy pomagające funkcjonariuszom zajmującym się oszustwami celnymi w wykrywaniu towarów importowanych, które należy poddać szczegółowej kontroli (rewizji). Zbadany został scenariusz[42] selekcji celnej z udziałem człowieka. Dane wprowadzane do modelu to formularze deklaracji importowych wymagane przez służby celne. Model selekcji zaznaczał towary, które jego zdaniem powinny zostać skontrolowane przez funkcjonariusza celnego, a funkcjonariusz przekazywał informację zwrotną do modelu selekcji, akceptując lub odrzucając zidentyfikowany przez model potencjalnie podejrzany formularz deklaracji. W przypadku uchylania się od płacenia podatków, a konkretnie uchylania się od płacenia ceł, kwestia dochodów uzyskanych dzięki kontroli i identyfikacji uchylania się od płacenia podatków była celem, który był brany pod uwagę w modelowaniu. Głównym modelem zastosowanym w badaniach m.in. Sundonga Kima był model DATE. Jest to drzewiasty model *dual-attentive*, który pozwala na optymalizację podwójnych celów. W tym przypadku podwójnymi celami były zarówno klasyfikacja nielegalnych transakcji, jak i predykcja zwrotu przychodów. Do poszukiwania najlepszego modelu w procesie selekcji wykorzystano strategię eksploracji oraz strategię eksploatacji. Strategia eksploracji jest definiowana jako podejście do wyboru niepewnych pozycji przy ryzyku natychmiastowej utraty przychodów, z potencjałem do wykrycia bardziej nowatorskich wzorców oszustw w przyszłości. Podejście eksploatacyjne stara się wybrać najbardziej prawdopodobne pozycje związane z oszustwami i wysokimi zyskami, aby zabezpieczyć krótkoterminowe dochody dla administracji celnej. Zestaw danych zebranych do tego eksperymentu

[41] Customs Fraud-EU Anti-Fraud Offce, <https://anti-fraud.ec.europa.eu/investigations/investigations-related-eu-revenue/investigating-customs-fraud_en>, 9 maja 2023 r.

[42] S. Kim i in., *Take a chance: Managing the exploitation-exploration dilemma in customs fraud detection via online active learning*, 2020, <https://arxiv.org/pdf/2010.14282.pdf>, 9 maja 2023 r.

wykorzystywał informacje z deklaracji importowych na poziomie transakcji trzech krajów afrykańskich. Deklaracje te były bardzo dokładne, łącznie z kwotami naliczonych ceł, ze względu na prawie 100% wskaźnik kontroli importowanych towarów. Zaimplementowano wiele technik hybrydowych, ale głównym modelem wykorzystanym w procesie selekcji był DATE, wykazujący najwyższą wydajność oceny.

Uchylanie się od podatków

Uchylanie się od opodatkowania to bezprawne działanie podatników polegające na celowym zaniechaniu płacenia zobowiązań podatkowych odpowiednim organom. Istnieje znaczna liczba badań, które miały miejsce w dziedzinie unikania podatków z zastosowaniem *deep learningu* i uczenia maszynowego, np. badania wykonane na bułgarskich podatnikach lub handlowcach[43], którzy nie wywiązywali się z obowiązku płacenia podatku VAT. Eksperymentując z zestawem danych bułgarskich podatników i handlowców, których łączna liczba wynosiła 312 726 osób, przy czym średnio 75% z nich przeprowadziło jedną transakcję finansową miesięcznie, badacze zidentyfikowali wysoki (rzędu 80) procent podatników/przedsiębiorców nieprzestrzegających przepisów w ramach bułgarskich deklaracji i ksiąg VAT.

SIM-Swapping

SIM-Swapping to atak, który pozwala cyberprzestępcy uzyskać nieautoryzowaną kontrolę nad numerem telefonu komórkowego klienta sieci bezprzewodowej. Daje to atakującemu dostęp do wiadomości tekstowych opartych na SMS-ach, które umożliwiają resetowanie haseł kont na stronach internetowych, które opierają się na bezpieczeństwie numeru telefonu komórkowego[44]. Udany atak SIM-Swap wymaga od aktora posiadania numeru telefonu celu oraz, w zależności od konta, do którego chce uzyskać dostęp, również jego adresu e-mail. Aktorzy albo skontaktują się z dostawcą usług ofiary i będą ją naśladować w celu przeniesienia numeru telefonu na nową kartę SIM albo mają współpracujących pracowników dostawcy usług, co pozwoli im na łatwiejszą drogę dostępu. Gdy aktor ma dostęp do numeru telefonu ofiary na własnej karcie SIM, może wydobyć wiadomości SMS, w tym hasła jednorazowe wysyłane przez serwisy finansowe czy banki. Schemat procesu SIM-Swap jest następujący:

Faza 1: Atakujący uzyskuje dostęp do danych uwierzytelniających konto ofiary i numerów telefonów komórkowych.

[43] A. Alexopoulos i in., *Detecting Network Anomalies in the Value Added Taxes (VAT) System*, <http://tarc.exeter.ac.uk/media/universityofexeter/businessschool/documents/centres/tarc/publications/reports/Detecting_Network_Anomalies_in_the_VAT_system.pdf>, 17 maja 2023 r.

[44] N. Andrews, *„Can I get your digits?": Illegal acquisition of wireless phone numbers for SIM-swap attacks and wireless provider liability*, "Northwestern Journal of Technology and Intellectual Property" 2018, Vol. 16, s. 79–106.

Faza 2: Atakujący manipuluje dostawcą usług, aby wykonać SIM-Swap z numerem telefonu komórkowego ofiary.

Faza 3: Korzystając z nowo uzyskanego dostępu, napastnik może teraz użyć danych uwierzytelniających do zainicjowania próby logowania do konta finansowego.

Faza 4: Dostawca usług finansowych wysyła hasło jednorazowe na numer telefonu komórkowego ofiary.

Faza 5: Zostaje uzyskany dostęp do konta finansowego ofiary, a środki są przenoszone i prane.

Badania naukowców zidentyfikowały trzy główne etapy przestępstwa wymiany karty SIM: 1) kradzież danych osobowych, 2) oszukańcze skopiowanie karty SIM oraz 3) wykorzystanie nieuczciwie uzyskanej usługi mobilnej do popełnienia przestępstwa. Badania wykazały również, że procedura uwierzytelniania abonenta związana z wymianą karty SIM jest narażona na kradzież tożsamości, zwłaszcza w krajach, które wdrożyły eSIM[45]. Istotna w tym typie przestępstwa była praca naukowców analizująca włamanie do sieci telefonii komórkowej T-Mobile w 2021 r., przeprowadzone przez Johna Erin Binnsa, które skutkowało kradzieżą danych osobowych 54 milionów klientów. Atakujący uzyskał dostęp do systemów fakturowych T-Mobile za pośrednictwem niezabezpieczonego właściwie routera i wykorzystał techniki *brute force*, aby uzyskać dostęp do poufnych informacji przechowywanych na wewnętrznych serwerach firmy. Skradzione dane obejmowały nazwiska, adresy, numery ubezpieczenia społecznego, daty urodzin, numery prawa jazdy, informacje identyfikacyjne, numery IMEI i IMSI. Wspomniana analiza przedstawiała, w jaki sposób pozyskanie powyższych danych otwiera drzwi do kradzieży tożsamości i wielu innych form hakowania, takich jak właśnie przejmowanie karty SIM[46]. Przeprowadzone zostały również badania dotyczące łatwości pozyskiwania numerów telefonów komórkowych za pośrednictwem różnych usług komunikacyjnych, takich jak WhatsApp, Signal i Telegram. W publikacji *All the numbers are U.S.: Large-scale abuse of contact discovery in mobile messengers*[47] autorzy opisali wykorzystanie metod wykrywania kontaktów z komunikatorów mobilnych i wydobywania telefonów komórkowych oraz sposoby pozyskania ich prywatnych danych. Poprzez kombinację ataków typu *crawling* i *hash reversal*, w ustalonym czasie i przy ograniczonych zasobach, naukowcy byli w stanie uzyskać 100% numerów telefonów komórkowych dla Signal, 10% dla WhatsAppa oraz ujawnić słabości API Telegram, ujawniając szeroki zakres wrażliwych informacji. Tego typu luki bezpieczeństwa

[45] M. Kim, J. Suh, H. Kwon, *A Study of the Emerging Trends in SIM Swapping Crime and Effective Countermeasures*, 2022 IEEE/ACIS 7th International Conference on Big Data, Cloud Computing, and Data Science (BCD), August 4–6 2022, Danang, Vietnam, <https://ieeexplore.ieee.org/document/9900510>, 17 maja 2023 r.

[46] C. Faircloth i in., *A Study on Brute Force Attack on T-Mobile Leading to SIM-Hijacking and Identity-Theft"* [w:] Proceedings of the 2022 IEEE World AI IoT Congress (AIIoT), Seattle, WA, USA, 6–9 June 2022, <https://ieeexplore.ieee.org/document/9817175>,17 maja 2023 r.

[47] C. Hagen i in., *All the numbers are U.S.: Large-scale abuse of contact discovery in mobile messengers* [w:] Proc. Netw. Distrib. Syst. Secur. Symp. (NDSS), 2021, s. 1–17, <https://encrypto.de/papers/HWSDS21.pdf>, 17 maja 2023 r.

i prywatności w aplikacjach do przesyłania wiadomości umożliwiają potencjalnym atakującym dostęp i identyfikację ofiar dla SIM-Swapping.

Phishing

Phishing jest uważany za technikę inżynierii społecznej (*social engieneering*), która polega na nakłonieniu ofiary do przekazania swoich danych osobowych, w tym haseł, adresów e-mail, numerów telefonów, adresów, nazw użytkownika i informacji finansowych[48]. Analizując zamieszczoną wcześniej tabelę 1, podaje się, że phishing i jego warianty tylko w 2022 r. doprowadziły w Stanach Zjednoczonych do strat rzędu 52 milionów dolarów. W 2020 r. opracowano narzędzie o nazwie SEADer++[49] służące do wykrywania ataków socjotechnicznych w środowiskach internetowych z wykorzystaniem uczenia maszynowego. System ten próbuje wykryć inżynierię społeczną ataków na podstawie NLP i sztucznych sieci neuronowych. Badacze oparli swoją koncepcję na próbie wykrycia ataku inżynierii społecznej w środowisku czatu *online*. Proponowany proces składał się z trzech etapów, którymi były: wstępne przetwarzanie danych, ekstrakcja cech oraz agregacja wyników. Agregacja wyników obejmowała technikę klasyfikacji w celu identyfikacji prób inżynierii społecznej. Badacze odnotowali wysoką dokładność wyników klasyfikacji przy użyciu drzewa decyzyjnego, lasu losowego i MLP. Na podstawie wyników AUC zaproponowana metoda *Soft-voting Ensemble Learning* została uznana za najlepsze rozwiązanie dla aplikacji przemysłowej. Zrozumienie psychologii stojącej za inżynierią społeczną i jej zdolności do manipulowania ludźmi może pomóc w walce z phishingiem. Jak widać, w narzędziu SEADer++, wykorzystano zasady perswazji i psychomanipulacji. W pracy *Human Cognition Through the Lens of Social Engineering Cyberattacks*[50] zaproponowano traktowanie cyberataków socjotechnicznych jako ataku psychologicznego oraz zasugerowano rozszerzenie standardowych ram ludzkiego poznania w celu rozpoznania i akomodacji cyberataków socjotechnicznych. Te ramy stworzone przez badaczy doprowadziły do ilościowego przedstawienia matematycznej charakterystyki perswazji. Praca ta pokazuje zakres nauki i badań niezbędnych do skutecznego zwalczania cyberataków socjotechnicznych skierowanych na przemysł i ludność cywilną.

Oszustwo na romans

Romance fraud według definicji FBI[51] to oszustwo, które ma miejsce, gdy przestępca przyjmuje fałszywą tożsamość *online*, aby zdobyć sympatię

[48] R. Alabdan, *Phishing attacks survey: Types, vectors, and technical approaches*, "Future Internet" 2020, Vol. 12, s. 1–39.

[49] M. Lansley i in., *SEADer++: Social engineering attack detection in online environments using machine learning*, "Journal of Information and Telecommunication" 2020, Vol. 4, No. 3, s. 346–362, <https://www.tandfonline.com/doi/full/10.1080/24751839.2020.1747001>, 17 maja 2023 r.

[50] R. Montañez, E. Golob, S. Xu, *Human cognition through the lens of social engineering cyberattacks*, "Frontiers in Psychology" 2020, Vol. 11, s. 1–18.

[51] FBI, Romance Fraud, <https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/romance-scams>, 17 maja 2023 r.

i zaufanie ofiary. Oszuści wykorzystują to zaufanie, aby zbudować iluzję romansu lub bliskiego związku oraz manipulować ofiarami w celu uzyskania korzyści finansowych. Tego typu oszustwo odnotowało wzrost popularności wśród przestępców szczególnie w wyniku globalnej blokady spowodowanej COVID-19 — z doniesieniami o nawet 20% wzroście oszustw związanych z przelewami bankowymi skojarzonymi z oszustwami romansowymi w 2020 r. w porównaniu z 2019 r. Ofiary nie tylko są okradane z własnych pieniędzy, ale mogą być wykorzystywane jako muły do prania pieniędzy, np. będąc proszone o przekazanie otrzymanych pieniędzy od aktora na różne konta, które on poleci. Niewiele jest publikacji dotyczących zwalczania oszustw na romans z wykorzystaniem technik uczenia maszynowego. W artykule *Automatically dismantling online dating fraud*[52] został przedstawiony system, który z dużą precyzją wykrywa oszustwa lub wyłudzenia na portalach randkowych, jednak w wynikach znalazło się wiele fałszywie negatywnych klasyfikacji, ponieważ okazuje się, że prawdziwe profile mają bardzo podobne cechy do fałszywych.

Ransomware

Ransomware jest formą złośliwego oprogramowania, które ma zdolność do szyfrowania systemów komputerowych i informacji cyfrowych ofiary, zabraniając dostępu do nich do czasu zapłacenia okupu napastnikom. *Malware* to złośliwe oprogramowanie, tworzone z intencją przestępczą w celu uzyskania dostępu w sposób niewykryty do systemów komputerowych swoich ofiar. Istnieją różne formy złośliwego oprogramowania, w tym konie trojańskie, rootkity i wirusy[53]. Typowa płatność żądana przez przestępców jest w kryptowalutach ze względu na anonimowość otaczającą właścicieli portfeli.

Ransomware jest wyrafinowaną metodą stosowaną przez cyberprzestępców finansowych. Jego popularność rośnie, co widać w ostatnich atakach — w 2021 r. na Colonial Pipeline w USA, Irish Health Service Executive oraz najwyższym w historii ataku *ransomware* na firmę Acer z żądaniem od cyberprzestępców zapłacenia 50 milionów dolarów. Od 50 do 75% ofiar *ransomware* to małe firmy[54]. *Ransomware* stanowi połączenie wcześniej omówionych metod w cyberprzestępczości finansowej. Jest to mieszanka prania pieniędzy w kryptowalutach i inżynierii społecznej w celu włamania się i uzyskania dostępu do korporacji, firm i instytucji. Środki zapobiegawcze w walce z *ransomware* obejmują poprawę bezpieczeństwa cybernetycznego dla potencjalnych ofiar oraz środki reaktywne,

[52] G. Suarez-Tangil i in., *Automatically dismantling online dating fraud*, "IEEE Transactions on Information Forensics and Security" 2019, Vol. 15, s. 1128–1137.

[53] W. Zakaria i in., *The rise of ransomware* [w:] CSEB '17: Proceedings of the 2017 International Conference on Software and e-Business, December 28–30, 2017, New York 2017, s. 66–70.

[54] L. Barr, *DHS Secretary Warns Ransomware Attacks on the Rise, Targets Include Small Businesses*, 6 May 2021, <https://abcnews.go.com/Politics/dhs-secretary-warns--ransomwareattacks-rise-targets-include/story?id=77512872>, 17 maja 2023 r.

takie jak te widoczne w artykułach na blogu Elliptic, gdzie można śledzić pieniądze i identyfikować organizacje przestępcze.

Deepfakes i GPT-4

Wraz z rozwojem modeli ML do przeciwdziałania cyberprzestępczości finansowej nastąpił postęp technologii, która ułatwia aktorom popełnianie przestępstw. *Deepfakes* i zaawansowane chatboty, takie jak GPT-4[55], są w stanie spoofować i zmanipulować pracowników na wszystkich szczeblach organizacyjnych. W marcu (jeszcze GPT-2) 2019 r. prezes firmy energetycznej z siedzibą w Wielkiej Brytanii wierzył, że rozmawia ze swoim zwierzchnikiem, prezesem spółki macierzystej z siedzibą w Niemczech. Był to w rzeczywistości wyrafinowany model *deepfake* wdrożony w celu dokonania przestępstwa przy wykorzystaniu inżynierii społecznej. Dzięki temu przestępcy zyskali około 250 000 euro. *Deepfakes* to nie tylko manipulacje dźwiękowe, ale również wizualne. Programy *deepfake* są w stanie tworzyć całkowicie fikcyjne tożsamości osób. Strony internetowe wykorzystują *Generative Adversarial Network* do tworzenia „osoby", a nawet generowania zmodyfikowanych wizerunków osób bez ich zgody[56]. Wizerunki te mogą być również wykorzystywane w profilach internetowych, które mogą podszywać się pod prawdziwych użytkowników takich stron jak serwisy randkowe czy portale społecznościowe.

GPT jest szkolony do przewidywania następnego słowa w zdaniu i pokazał, że może tworzyć podobne do ludzkich fragmenty tekstu, takie jak artykuły informacyjne. GPT został wykorzystany do tworzenia fałszywych recenzji dla stron sprzedawców, takich jak np. Amazon. Fałszywe recenzje mogą oszukać prawdziwych klientów i skłonić ich do zawarcia transakcji z nielegalnymi dostawcami lub producentami towarów niskiej jakości, a także zaszkodzić całkowitemu wynikowi recenzji i reputacji konkurencyjnej firmy. „Ręczne" pisanie komentarzy na stronach sprzedawców jest metodą znaną jako *crowdturfing* i jest uważane za atak na systemy recenzji online.

Wyzwania i kierunki

Walka z cyberprzestępczością finansową nie jest łatwym zadaniem. Cyberprzestępcy finansowi (aktorzy) są wyrafinowani w swoich metodach ataku i przebiegli w posługiwaniu się metodami inżynierii społecznej. Chociaż badania posuwają się naprzód, dla specjalistów ds. cyberbezpieczeństwa jest to stale walka o byt. Poniżej przedstawiamy wyzwania i potencjalne przyszłe obszary badawcze, nad którymi należy pracować.

[55] To multimodalny duży model językowy stworzony przez OpenAI i czwarty z numerowanej serii „GPT-n" podstawowych modeli GPT, <https://en.wikipedia.org/wiki/GPT-4>, 17 maja 2023 r.

[56] Random Face Generator (This Person Does Not Exist), <https://this-person-does-not-exist.com/en>, 17 maja2023 r.

Tworzenie praktycznych i efektywnych technik uczenia maszynowego lub głębokiego uczenia wymaga nie tylko dokładności w przewidywaniach, ale także szybkości. Szczególnie w dziedzinie finansów klienci oczekują, że transakcje zostaną bezproblemowo dostarczone do odpowiednich odbiorców. Ambicja wdrożenia aplikacji w świecie rzeczywistym w tej branży wymaga zdolności do aktualizacji bazowych zbiorów danych w odpowiedzi na nowe transakcje w czasie rzeczywistym, bez zbędnych opóźnień.

Pojawienie się kryptowalut w połączeniu z wykorzystaniem DarkNetu i powiązanych narzędzi maskujących IP, takich jak VPN, utrudnia zadanie identyfikacji cyberprzestępców finansowych. Metody wykrywania kont mieszających kryptowaluty są kluczowe na etapie maskowania, prania kryptowalut. Kluczowym obszarem badań dla prania kryptowalut jest strategia wyjścia stosowana przez przestępców. Aby móc zamienić kryptowalutę na bardziej korzystną walutę, istnieje szereg metod obejmujących korzystanie z dostawców rynku pochodzących z DarkNetu, którzy akceptują transakcje kryptowalutowe w zamian za inną fizyczną walutę. Inne metody obejmują bardziej powszechnie stosowane giełdy, takie jak *Coinbase* czy rynki wymiany w DarkNecie, takie jak Hydra dla kart upominkowych i bonów, które mogą być używane do zakupu dóbr materialnych. Hydra, rosyjskie targowisko w DarkNecie, otrzymało w 2020 r. bitcoiny o wartości ponad 1,4 miliarda dolarów. W zamian za bitcoina użytkownik otrzymuje przedpłacone karty debetowe. Wspólną cechą wszystkich metod jest przemieszczanie kryptowaluty z jednego portfela do drugiego, a tym samym rejestrowanie identyfikowalnej transakcji w blockchainie. Identyfikacja tych kont/transakcji to krok w dobrym kierunku w zwalczaniu metod w demaskowaniu działalności oszustów. Konieczne jest bardziej szczegółowe wykorzystanie wykrywania anomalii opartych na grupach/grafach, aby zająć się strukturami społeczności w sieciach.

Tworzenie algorytmów do walki z przestępcami, którzy celowo ukrywają swoje działania, wymaga solidności. Ta solidność modelu może być zidentyfikowana i zmierzona poprzez jego słabości. Wyzwaniem przy projektowaniu metody zapobiegania działalności przestępczej jest również utrzymanie jej w stanie aktualizowania się wraz z działalnością przestępczą i wyrafinowanymi technikami. Aby rozwiązać ten problem, przyszłe badania powinny obejmować ataki, które będą próbowały przeniknąć do modelu, starając się uniknąć wykrycia przez algorytmy. Dzięki testom można zidentyfikować słabe punkty, a następnie zająć się nimi poprzez dalsze eksperymentowanie z modelem lub ponowną ocenę całego algorytmu. Solidność modelu obejmuje jego zdolność do adaptacji do zmian w danych i zmian cech. Są one powszechne w dziedzinie finansów ze względu na zmiany trendów ekonomicznych, nawyków wydatkowych klientów oraz wprowadzanie nowoczesnych technologii.

Ze względu na heterogeniczne właściwości kryptowalut, modelowanie ich w postaci grafu jest wyzwaniem. Ethereum i bitcoin mają różne struktury blockchain, gdzie ethereum jest w stanie włączyć kontrakty do swoich transakcji, podczas gdy bitcoin jest prostszą metodą transakcji, ale istnieje wciąż wiele sposobów reprezentacji węzłów i krawędzi na etapie

budowy grafu. Te różne formy reprezentacji wymagają od użytkownika zbudowania konkretnego grafu, aby uchwycić informacje o transakcjach niezbędne do wykonania zadania końcowego, takiego jak pranie pieniędzy lub być może analiza płynności zaległych kontraktów w sieci.

Metody wykrywania oszustw finansowych muszą działać na podstawie niepełnych i niepewnych danych. Ponieważ etykiety prawdy materialnej są poszukiwane poprzez ręczny przegląd przez analityków, zaktualizowany model oszustwa może być przestarzały z powodu opóźnienia w dostępności w czasie rzeczywistym bogatych danych incydentalnych. Wyzwaniem jest, aby systemy ML adaptowały się i podejmowały decyzje, opierając się na niekompletnych danych. Na przykład w typowym przypadku użycia AML nie każda obserwacja i ukryte zależności są dostępne w czasie podejmowania decyzji. To sprawia, że projektowanie i ocena algorytmów jest wyzwaniem. Metody samokontroli mają potencjalnie ogromny wpływ na przyszłość badań nad zwalczaniem cyberprzestępczości finansowej. Samoobsługowe podejścia do uczenia grafów mogą pozwolić nam na zrozumienie i prognozowanie zdarzeń bez uprzedzeń. Istnieje potencjalny przypadek użycia poprzez adaptację predykcji ruchu DeepMind, która wykorzystuje zaawansowane sieci neuronowe grafów i przekształca je dla sieci finansowych w celu identyfikacji złośliwych użytkowników.

Podsumowanie

Analizując najnowsze algorytmy, modele i techniki wykorzystywane do zwalczania różnych aspektów cyberprzestępczości finansowej, można stwierdzić, że nie jest to zadanie trywialne. Sposób obfuskacji, manipulacji i maskowania zachowań stwarza trudne zadanie dla badaczy i inżynierów, którzy muszą doprowadzić do identyfikacji i wykrywania złośliwego, nielegalnego działania oraz zapobiec mu. Jak widać w literaturze, wykrywanie anomalii grupowych, głębokie uczenie i teoria grafów są łączone w celu identyfikacji sieci złośliwych aktorów w ramach ogólnych grup użytkowników i klientów. Przy dużych sumach pieniędzy wydobywanych z systemu finansowego, istnieje kara płacona przez społeczeństwo poprzez wzrost opłat i brak zaufania do ich prywatnych informacji przechowywanych przez firmy. Można stwierdzić, że cyberprzestępczość finansowa ma wpływ na nasze społeczeństwo na poziomie socjologicznym, szczególnie w obszarze prania pieniędzy i unikania podatków. Brak konsekwencji lub odpłaty za działalność przestępczą może zakłócić i wywołać dyskoordynację w postrzeganiu policji przez społeczeństwo.

Bibliografia

1. Aggarwal C.C., *Outlier analysis in Data Mining*, Cham 2015.
2. Ahmed M., Mahmood A.N., Islam M.R., *A survey of anomaly detection techniques in financial domain*, "Future Generation Computer Systems" 2016, Vol. 55.

3. Alabdan R., *Phishing attacks survey: Types, vectors, and technical approaches*, "Future Internet" 2020, Vol. 12.
4. Alarab I., Prakoonwit S., Nacer M., *Competence of graph convolutional networks for anti-money laundering in bitcoin blockchain* [w:] *ICMLT '20: Proceedings of the 2020 5th International Conference on Machine Learning Technologies*, 19–21 June 2020, New York 2020.
5. Alexopoulos A. i in., *Detecting Network Anomalies in the Value Added Taxes (VAT) System*, <http://tarc.exeter.ac.uk/media/universityofexeter/businessschool/documents/centres/tarc/publications/reports/Detecting_Network_Anomalies_in_the_VAT_system.pdf>, 17 maja 2023 r.
6. Alhir S.S., *UML. Wprowadzenie*, Gliwice 2004.
7. AML/CFT, <https://www.gov.pl/web/finance/aml-cft>, 9 maja 2023 r.
8. Andrews N., *„Can I get your digits?": Illegal acquisition of wireless phone numbers for SIM-swap attacks and wireless provider liability*, "Northwestern Journal of Technology and Intellectual Property" 2018, Vol. 16.
9. Barr L., *DHS Secretary Warns Ransomware Attacks on the Rise, Targets Include Small Businesses*, 6 May 2021, <https://abcnews.go.com/Politics/dhs-secretary-warns-ransomwareattacks-rise-targets-include/story?id=77512872>, 17 maja 2023 r.
10. Blondel V. i in., *Fast unfolding of communities in large networks*, "Journal of Statistical Mechanics: Theory and Experiment" 2008, Vol. 2008.
11. Carding, <https://en.wikipedia.org/wiki/Carding_(fraud)>, 9 maja 2023 r.
12. Chalapathy R., Chawla S., *Deep learning for anomaly detection: A survey*, 2019, <https://www.researchgate.net/publication/330357393_Deep_Learning_for_Anomaly_Detection_A_Survey>, 19 października 2023 r.
13. Cook A.A., Misirli G., Fan Z., *Anomaly Detection for IoT Time-Series Data: A Survey*, "IEEE Internet Things Journal" 2020, No. 7.
14. *Crypto Crimes & Anti-Money Laundering (AML) Report March 2023*, <https://ciphertrace.com/crime-and-anti-money-laundering-report-march-2023/>, 9 maja 2023 r.
15. Customs Fraud-EU Anti-Fraud Offce, <https://anti-fraud.ec.europa.eu/investigations/investigations-related-eu-revenue/investigating-customs-fraud_en>, 9 maja 2023 r.
16. Dark web (net), ciemna sieć, <https://pl.wikipedia.org/wiki/Dark_web>, 9 maja 2023 r.
17. Darvishi H. i in., *Sensor-fault detection, isolation and accommodation for digital twins via modular data-driven architecture*, "IEEE Sensors Journal" 2021, Vol. 21, No. 4.
18. Dreżewski R., Sepielak J., Filipkowski W., *The application of social network analysis algorithms in a system supporting money laundering detection*, "Information Sciences" 2015, Vol. 295.
19. Erfani S.M. i in., *Highdimensional and large-scale anomaly detection using a linear one-class SVM with deep learning*, "Pattern Recognition" 2016, Vol. 58.
20. Europol, <https://www.europol.europa.eu>, 28 marca 2023 r.
21. Europol, Economic Crime, <https://www.europol.europa.eu/crime-areas/economic-crime>, 19 października 2023 r.
22. Faircloth C. i in., *A Study on Brute Force Attack on T-Mobile Leading to SIM-Hijacking and Identity-Theft"* [w:] Proceedings of the 2022 IEEE World AI IoT Congress (AIIoT), Seattle, WA, USA, 6–9 June 2022, <https://ieeexplore.ieee.org/document/9817175>,17 maja 2023 r.
23. FBI, *Internet Crime Report 2022*, <https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf>, 19 kwietnia 2023 r.
24. FBI, Romance Fraud, <https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/romance-scams>, 17 maja 2023 r.
25. *Fighting Financial Crime With AI*, <https://www.ibm.com/downloads/cas/WKLQKD3W>, 29 marca 2023 r.
26. Gaihre A., Pandey S., Liu H., *Deanonymizing cryptocurrency with graph learning: The promises and challenges* [w:] *2019 IEEE Conference on Communications and Network Security*, Washington, 10–12 June 2019.
27. GPT-4, <https://en.wikipedia.org/wiki/GPT-4>, 17 maja 2023 r.
28. Hagen C. i in., *All the numbers are U.S.: Large-scale abuse of contact discovery in mobile messengers* [w:] Proc. Netw. Distrib. Syst. Secur. Symp. (NDSS), 2021, <https://encrypto.de/papers/HWSDS21.pdf>, 17 maja 2023 r.
29. Hasham S., Joshi S., Mikkelsen D., *Financial Crime and Fraud in the Age of Cybersecurity*, Shanghai 2019.

30. Kim M., Suh J., Kwon H., *A Study of the Emerging Trends in SIM Swapping Crime and Effective Countermeasures*, 2022 IEEE/ACIS 7th International Conference on Big Data, Cloud Computing, and Data Science (BCD), August 4–6 2022, Danang, Vietnam, <https://ieeexplore.ieee.org/document/9900510>, 17 maja 2023 r.
31. Kim S.i in., *Take a chance: Managing the exploitation-exploration dilemma in customs fraud detection via online active learning*, 2020, <https://arxiv.org/pdf/2010.14282.pdf>, 9 maja 2023 r.
32. Lansley M. i in., *SEADer++: Social engineering attack detection in online environments using machine learning*, "Journal of Information and Telecommunication" 2020, Vol. 4, No. 3, <https://www.tandfonline.com/doi/full/10.1080/24751839.2020.1747001>, 17 maja 2023 r.
33. Metcalfe A.V., Cowpertwait P.S., *Introductory Time Series With R*, New York 2009.
34. Męczkowska-Christiansen A., Charuta-Kojkoł J., Zacniewska J., *Computational thinking on the background of the theory of mind and didactic strategies of its development,* „Colloquium" 2021, t. 13, nr 4.
35. Monero, <https://pl.wikipedia.org/wiki/Monero>, 9 maja 2023 r.
36. *Money Laundering Offences*, <https://www.legislation.gov.uk/ukpga/2002/29/part/7>, 19 kwietnia 2023 r.
37. Montañez R., Golob E., Xu S., *Human cognition through the lens of social engineering cyberattacks*, "Frontiers in Psychology" 2020, Vol. 11.
38. Obfuskacja — zaciemnianie kodu, <https://pl.wikipedia.org/wiki/Zaciemnianie_kodu dostęp>, 9 maja 2023 r.
39. Opitek P., *Przeciwdziałanie praniu pieniędzy z wykorzystaniem walut wirtualnych w świetle krajowych i międzynarodowych regulacji AML*, „Prokuratura i Prawo" 2020, nr 12.
40. OPSEC, <https://en.wikipedia.org/wiki/Operations_security>, 19 kwietnia 2023 r.
41. Random Face Generator (This Person Does Not Exist), <https://this-person-does-not-exist.com/en>, 17 maja 2023 r.
42. Suarez-Tangil G. i in., *Automatically dismantling online dating fraud*, "IEEE Transactions on Information Forensics and Security" 2019, Vol. 15.
43. Światowe Forum Ekonomiczne, <https://pl.wikipedia.org/wiki/%C5%9Awiatowe_Forum_Ekonomiczne>, 28 marca 2023 r.
44. Toth E., Chawla S., *Group deviation detection methods: A survey*, "ACM Computing Surveys" 2018, Vol. 51, No. 4.
45. *Unified Modeling Language*, <https://pl.wikipedia.org/wiki/Unified_Modeling_Language>, 19 kwietnia 2023 r.
46. Ustawa z 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (tekst jedn. DzU z 2023 r., poz. 1124).
47. Wang Q.i in., *Enhancing intraday stock price manipulation detection by leveraging recurrent neural networks with ensemble learning*, "Neurocomputing" 2019, Vol. 347, <https://doi.org/10.1016/j.neucom.2019.03.006>, 19 kwietnia 2023 r.
48. Wu Z. i in., *A comprehensive survey on graph neural networks*, "IEEE Transactions on Neural Networks and Learning Systems 2021, Vol. 32, No. 1.
49. X. Song i in., *Conditional anomaly detection*, "IEEE Transactions on Knowledge and Data Engineering" 2007, Vol. 19, No. 5.
50. Zakaria W. i in., *The rise of ransomware* [w:] CSEB '17: Proceedings of the 2017 International Conference on Software and e-Business, December 28–30, 2017, New York 2017.
51. Zhou Y. i in., *Analyzing and detecting money-laundering accounts in online social networks*, "IEEE Network" 2018, Vol. 32, No. 3.
52. <https://pl.wikipedia.org/wiki/Tor_(sieć_anonimowa)>, 19 kwietnia 2023 r.
53. <https://pl.wikipedia.org/wiki/Wirtualna_sieć_prywatna>,19 kwietnia 2023 r.
54. <https://us.norton.com/blog/emerging-threats/what-is-bulletproof-hosting#>, 19 kwietnia 2023 r.

DOI: 10.5604/01.3001.0053.9746
http://dx.doi.org/ 10.5604/01.3001.0053.9746

Słowa kluczowe: sztuczna inteligencja, wykrywanie zagrożeń, analiza behawioralna, zapobieganie oszustwom, wykrywanie phishingu, wykrywanie złośliwego oprogramowania, zarządzanie lukami w zabezpieczeniach, reagowanie na incydenty, wykrywanie zagrożeń, analityka predykcyjna, automatyzacja bezpieczeństwa

Streszczenie: Zwalczanie cyberprzestępczości gospodarczej za pomocą sztucznej inteligencji może być skutecznym nowym podejściem. Technologie sztucznej inteligencji mogą bowiem wykrywać cyberzagrożenia i reagować na nie w czasie rzeczywistym, identyfikować wzorce i anomalie w dużych zbiorach danych oraz automatyzować różne procesy bezpieczeństwa. Podstawowe sposoby wykorzystania sztucznej inteligencji do zwalczania cyberprzestępczości ekonomicznej to wykrywanie zagrożeń, analiza behawioralna, zapobieganie oszustwom, wykrywanie phishingu i złośliwego oprogramowania, zarządzanie lukami w zabezpieczeniach, reagowanie na incydenty i wykrywanie zagrożeń, analityka predykcyjna czy automatyzacja bezpieczeństwa. Należy jednak zauważyć, że chociaż sztuczna inteligencja może znacznie usprawnić działania związane z cyberbezpieczeństwem, nie jest to samodzielne rozwiązanie. Należy go używać w połączeniu z innymi środkami bezpieczeństwa, takimi jak regularne aktualizacje oprogramowania, szkolenia pracowników i silne kontrole dostępu, aby stworzyć solidną obronę przed cyberprzestępczością ekonomiczną.