Ministerstwo Cyfryzacji

Departament Cyberbezpieczeństwa

TLP:GREEN

BIULETYN INFORMACYJNY

ZAGROŻENIA W CYBERPRZESTRZENI

07/2024

SPIS TREŚCI

Wzrost aktywności azjatyckich grup APT

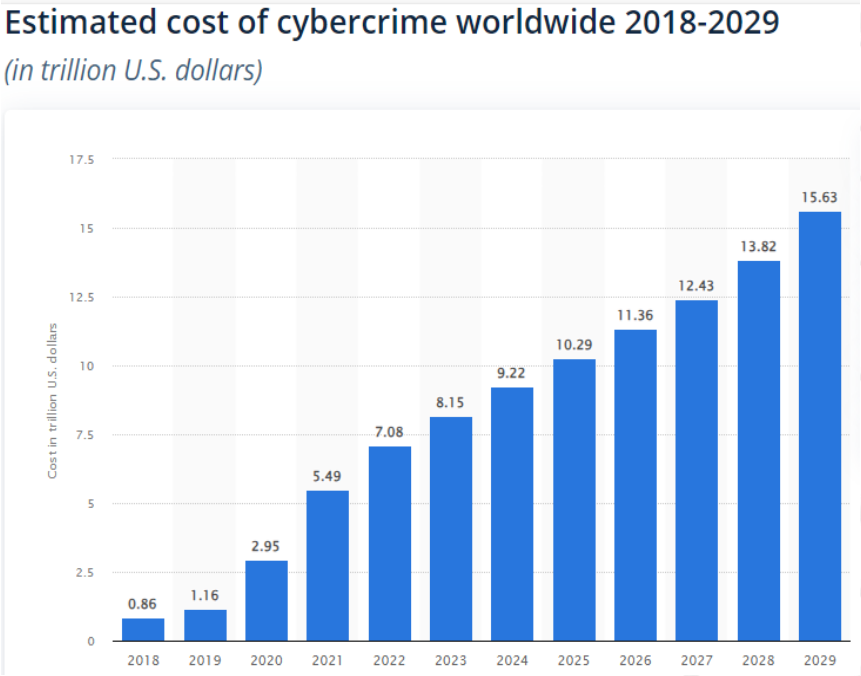
Pod koniec lipca br. amerykańska CISA opublikowała poradnik dotyczący przeciwdziałania złośliwej aktywności grup APT (*Advanced Peresistent Threat*) powiązanych z administracją Korei Północnej (KRLD). Materiał jest wytworem współpracy podmiotów amerykańskich, brytyjskich oraz południowo koreańskich. Te szczegółowe kompendium wiedzy, poza zestawieniem wykorzystywanego arsenału technicznego i *modus operandi* służb Kim Dzong Una, opisuje cele ich ataków. Analiza materiału ukazuje, jak sterowana przez Pjongjang grupa *RGB 3rd Bureau* (znana również jako: *Andariel, Onyx Sleet, PLUTONIUM, DarkSeoul, Silent Chollima, i Stonefly/Clasiopa)* wykorzystuje przestrzeń cyfrową do prowadzenia działalności wywiadowczej skupionej na pozyskiwaniu wiedzy technologicznej, gospodarczej i naukowej. Do obszarów zaliczonych w zakres podstawowych celów ataków włączono podmioty z przemysłu obronnego (*m.in. sprzęt ciężki, okręty podwodne, pojazdy autonomiczne*), lotniczego (*m.in. samoloty i bezzałogowe statki powietrzne, pociski rakietowe i technologie satelitarne*), jądrowego (*m.in. przetwarzanie uranu, zarządzanie odpadami, energetyka jądrowa)* i inżynieryjnego (*m.in. budownictwo okrętowe i morskie, roboty przemysłowe, przetwórstwo metali*). Zgodnie z ww. poradnikiem, analitycy z CISA stwierdzają, że celem ataków koreańskich służb wywiadowczych, są dane i informacje dot. m.in. specyfikacji kontraktów, zestawienia materiałów, szczegóły projektowe, rysunki architektoniczne i dokumenty inżynieryjne – mające zastosowanie cywilne i wojskowe. Inaczej wszystko to, co jest związane z tematyką obronności oraz rozwojem programów jądrowych, i mieści się w grupie żywotnych interesów totalitarnej władzy reżimu Kima.

Kim Dzong Un fot. PAP/EPA/KCNA

Zdobycie zasobów wiedzy w obszarach tak intratnych, wysokokosztowych i wrażliwych, jak te z ww. grup byłoby nie tylko poza zasięgiem i potencjałem krajowych ośrodków naukowo-badawczych, ale również i poza możliwościami operacyjnymi klasycznych służb wywiadowczych większości państw świata, w tym przede wszystkim tych, będących na granicy zaliczenia do krajów upadłych.

Powyższe obrazuje wysoką efektywność kosztową i wskazuje kluczowe znaczenie kradzieży własności intelektualnej w cyberprzestrzeni dla stworzenia warunków rozwoju technologicznego państw autorytarnych. Działalność cyber-szpiegowska umożliwia państwom o izolacjonistycznych reżimach utrzymanie się w technologicznym peletonie w wyścigu rozwojowym napędzanym przez naturalny postęp technologiczno-cywilizacyjny państw Zachodu.

Nawet uproszczone kalkulacje oparte o dane z rynku cywilnego dot. utworzenia dużego komercyjnego zespołu badaczy bezpieczeństwa teleinformatycznego - pentesterskiego/red-team'owego (którego specyfika i metodologia pracy wykorzystuje ten same narzędzia i know-how co grupy APT), złożonego z dwudziestu najwyższej klasy krajowych specjalistów (nie licząc personelu administracyjno-logistycznego), stwierdzają iż roczny koszt to ok. 5 milionów złotych. W sytuacji, gdy mowy o systemach kluczowych dla obronności państwa, należy użyć stosownego porównania – tj. wartość równoznaczna z... 5 sztukami lekkiego pojazdu opancerzonego klasy *Humvee* lub z ok. 100-150 pociskami artyleryjskimi 155mm. Dla uzmysłowienia skali kosztowej działań wojennych, Ukraina w trakcie trwającego konfliktu zbrojnego zużywa ok. 7 tys. pocisków tej klasy na dobę.



Szacunkowe światowe koszty przestępstw internetowych (łącznie z wywiadem naukowo-technicznym). Źródło: Statista.com

Już w 2022 r. firma *Cybereason* w swoim raporcie informowała, że tylko jedna chińska grupa APT-41 (inaczej: *WInti*, *BARIUM*, *Blackfly*), wspierana przez Państwo Środka wykradała wartość intelektualną z ok. 30 zachodnich, międzynarodowych firm z sektora produkcyjnego, energetycznego i farmaceutycznego wyceną przekraczającą bilion dolarów (wg GUS całość polskich wydatków w 2022 r. na B+R wynosiło ok. 0.01% tej kwoty tj. ok. 10 mld. dol.). W skład tej wartości wchodzą koszty wytworzenia technologii, utrzymania infrastruktury oraz środki przeznaczone na badania i rozwój celem ich uzyskania.

Powyższe jest powodem zintensyfikowania wysiłków państw Zachodu celem przeciwdziałania szpiegowskiej aktywności krajów Azji Południowo-Wschodniej. Obserwowany w ostatnich latach skokowy rozwój technologiczny państw o autorytarnych reżimach, związany jest bezpośrednio ze wzmożoną aktywnością lokalnych służb specjalnych w cyberprzestrzeni. Służby te pozyskane technologie przekazują krajowym kompleksom naukowo-badawczym, a następnie zostają one dostosowane i zaimplementowane w procesy badawczo-produkcyjne z zamiarem wytworzenia własnych rozwiązań technologicznych. W dużej mierze opartych na dorobku naukowym i finansowym placówek badawczych z Zachodu. Proceder ten radykalnie zmniejsza koszty wytwarzania i komercjalizacji azjatyckich technologii, co ma bezpośredni wpływ na rentowność i konkurencyjność wprowadzanych rozwiązań oraz prac badawczo-rozwojowych z Zachodu.

Jak błąd CrowdStrike'a został zaadaptowany przez hakerów

W nocy z 18 na 19 czerwca br. świat zamarł - częściowo dosłownie. Po godzinie 21.40 tysiące komputerów (łącznie ponad 8,5 mln urządzeń) z sytemem operacyjnym Windows zaczęła zalewać fala "niebieskich ekranów śmierci" (tzw. *bluescreen of death*), a setki lokalnych administratorów zostało wybudzonych ze snu celem naprawy oprogramowania. Tego dnia zdiagnozowano dwie krytyczne awarie kluczowych systemów teleinformatycznych. Pierwsza, to usterka *data center* usług chmurowych *Microsoft Azure USA*. Druga, to błędna konfiguracja automatycznej aktualizacji podsystemu antywirusowego *Falcon Sensor*, wchodzącego w skład holistycznych rozwiązań bezpieczeństwa cyfrowego dostarczanych przez firmę *CrowdStrike*.

Źródło: securityweek.com/

Skala incydentów oraz charakter podmiotów dotkniętych awarią (m.in. infrastruktura krytyczna i inne podmioty kluczowe, tj. lotniska, szpitale, strategiczne zakłady energetyczne oraz przemysłowe), powodowały skojarzenie z 2020 r. i z rosyjskim atakiem hakerskim na cyfrowy łańcuch dostaw w postaci usług *Orion* firmy *SolarWinds*. *CrowdStrike* oraz *Microsoft* szybko zdementowały plotki o ataku i opublikowały niezbędne poprawki bezpieczeństwa.

Niestety, w przeciwieństwie do pozytywów, złe wieści niosą się szybciej oraz docierają głębiej do świadomości odbiorców o czym doskonale wiedzą specjaliści od socjotechniki z grup cyberprzestępczych. Jak informuje *CrowdStrike*, już po kilku godzinach pojawiły się kampanie reklamowe fałszywych domen podszywających się pod oficjalne kanały publikujące aktualizację i dystrybuujące paczki poprawek do *FalconSensor*, oferując jednocześnie implant złośliwego oprogramowania – *HijackLoader'a* prowadzący do utraty dostępu do konta użytkownika.

Innym atakiem praktycznie natychmiast aktywowanym przez przestępców była kampania dystrybucji fałszywego podręcznika manualnej aktualizacji poprawek podszywająca się pod publikację *Microsoft*. Włączenie *makr* pobranego dokumentu uruchomiało wcześniej niezidentyfikowanego złośliwego *stealer'a* wstępnie nazwanego *Daolpu*.

Na fali zasięgów noszonego przez algorytmy wyszukiwarek i socialmediów hasła "*CrowdStrike*" chciały również wybić się grupy haktwistów. 24 lipca ugrupownie *USDoD* poinformowało o dokonaniu kradzieży danych z *CrowdStrike*, publikując listę (plik *.csv*) zawierającą informacje nt. rzekomo sklasyfikowanych przez firmę cyberprzestępców i podmiotów zaangażowanych w szkodliwą działalność cyfrową.

Komentarz:
Komunikując się w sprawie awarii oprogramowania, należy kontaktować się wyłącznie za pośrednictwem oficjalnych przedstawicieli rozwiązań, przy użyciu dedykowanych kanałów oraz przestrzegając wskazówek technicznych dostarczonych wyłącznie przez zespoły wsparcia producenta.

Strategicznie o cyberbezpieczeństwie – prezydenckie rekomendacje

Planowane jest opracowanie nowej Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, gdyż poprzednia wersja dokumentu z 2020 r. straciła na swojej aktualności w związku z daleko idącymi zmianami w środowisku bezpieczeństwa. Stosowanie do trybu przewidzianego w ustawie o obronie Ojczyzny, swoje rekomendacje do Strategii przedstawił prezydent RP. W następnym kroku za opracowanie Strategii odpowiada rząd, a finalnie zostanie ona zatwierdzona przez prezydenta. Przyjrzymy się, co o cyberbezpieczeństwie mówią prezydenckie rekomendacje.

Logo BBN.

Wśród 16 celów strategicznych proponowanych przez głowę państwa znalazł się cel mówiący o zapewnieniu proaktywnej obrony i ochrony przed zagrożeniami w nowych domenach, w tym m.in. w cyberprzestrzeni, w przestrzeni informacyjnej i kognitywnej. Z kolei w rekomendacjach poświęconych cyberbezpieczeństwu znajdziemy następujące inicjatywy:

- Rozwijać aktywną obronę w obszarze cyberbezpieczeństwa.
- Zwiększyć współpracę kontrwywiadowczą oraz technologiczną w ramach NATO i UE.
- Wzmacniać bezpieczeństwo sieci i systemów teleinformatycznych.
- Wprowadzić regulacje prawne zobowiązujące wszystkich operatorów usług kluczowych – bez względu na ich strukturę własności – do uczestnictwa w krajowych ćwiczeniach ochrony cyberprzestrzeni, przeprowadzania stress-testów i weryfikacji zabezpieczeń oraz przekazywania ich wyników organom odpowiedzialnym za cyberbezpieczeństwo państwa.
- Przygotować transsektorowy program rządowy dotyczący zwiększania narodowych zdolności w zakresie kryptologii, wytwarzania urządzeń komunikacyjnych, w tym kryptograficznych złożonych z produkowanych w Polsce komponentów i własnego oprogramowania oraz zagwarantować autonomię i bezpieczeństwo w zakresie komunikacji i transmisji danych dla operatorów infrastruktury krytycznej oraz w sektorze kosmicznym. Stworzyć bezpieczne środowisko informatyczne dla łączności i transmisji cyfrowych w warunkach z ograniczonym dostępem do globalnych sieci komunikacyjnych i nawigacyjnych.
- Podjąć działania mające na celu budowę krajowych kwantoodpornych rozwiązań kryptograficznych w odpowiedzi na rozwój technologii kwantowych.
- Kontynuować działania mające na celu odejście od wykorzystywania technologii pochodzących z państw uznawanych za autorytarne lub nieprzyjazne.
- Realizować działania w zakresie edukacji i zwiększania świadomości obywateli w obszarze higieny cyfrowej i cyberzagrożeń.

- Opracować i wdrożyć narodowy program badań i rozwoju w zakresie cyberbezpieczeństwa i sztucznej inteligencji.

W dokumencie jest też osobna część dotycząca przestrzeni informacyjnej, co jest zgodne z konstrukcją obecnej Strategii Bezpieczeństwa Narodowego RP, rozdzielając kwestie cyberbezpieczeństwa i bezpieczeństwa przestrzeni informacyjnej. Jest to też zgodne z logiką funkcjonowania Krajowego Systemu Cyberbezpieczeństwa i rozumienia cyberbezpieczeństwa w myśl ustawy o krajowym systemie cyberbezpieczeństwa. Niemniej w części poświęconej przestrzeni informacyjnej znajdziemy też ciekawe wątki pośrednio dotykające cyberbezpieczeństwa, takie jak:

- Zapewnić jednolitą komunikację strategiczną państwa.
- Wzmocnić oraz rozwinąć instrumenty do szybkiej analizy zagrożeń, predykcji działań adwersarzy oraz zdolności do aktywnego oddziaływania na przestrzeń informacyjną przeciwnika.
- Zdefiniować obszary przestrzeni informacyjnej RP, które powinny podlegać szczególnej ochronie ze strony państwa.
- Opracować strategię przeciwdziałania wrogim działaniom kognitywnym i budowania odporności kognitywnej państwa oraz znowelizować przepisy prawa w celu zapewnienia efektywnej i skoordynowanej obrony polskiej przestrzeni informacyjnej.

Warto zwrócić też uwagę na jedną z rekomendacji w części dotyczącej kierowania bezpieczeństwem narodowym. Proponuje się tam dokonać pilnego wyboru systemu łączności (spośród rozproszonych, funkcjonujących w sferze cywilnej i wojskowej systemów) oraz wdrożyć go na potrzeby zintegrowanego systemu łączności do kierowania bezpieczeństwem narodowym, w tym kierowania obroną państwa. Autorzy dokumentu przywołują, iż mimo zadań zapisanych w Strategii Bezpieczeństwa Narodowego RP z 2020 r. oraz wniosków z ćwiczeń TTX (podczas których weryfikowano system łączności niejawnej pomiędzy najważniejszymi organami w państwie w sytuacji zagrożenia konfliktem militarnym) nie zrealizowano prac zmierzających do zapewnienia bezpiecznej komunikacji na potrzeby kierowania bezpieczeństwem narodowym.

Ponadto ważny jest wątek jednej z rekomendacji w części dotyczącej przemysłowego sektora obrony i bezpieczeństwa. Mówi się, że tam, że należy wspierać wysiłki polskich podmiotów naukowo-badawczych na rzecz polskiego przemysłu obronnego, tj. należy powiązać działalność ośrodków naukowo-badawczych w zakresie badań i rozwoju w obszarze bezpieczeństwa, nadając im kierunki i priorytety w zakresie tworzenia nowoczesnych rozwiązań i technologii, w szczególności w obszarze cyberbezpieczeństwa, satelitarnych systemów rozpoznania, systemów bezzałogowych, rozwoju nowych i przełomowych technologii (EDT), w tym AI oraz technologii kwantowych.

Cyberbezpieczeństwo będzie niewątpliwie ważnym elementem nowej Strategii Bezpieczeństwa Narodowego RP. Jednocześnie trwają też pracę nad Strategią Cyberbezpieczeństwa RP na lata 2025-2029, co wynika z ustawy o krajowym systemie cyberbezpieczeństwa.

Źródło: BBN.

Rosyjskie działania na rzecz suwerenności technologicznej

Współcześnie niezwykle ważnym aspektem suwerenności państwa jest wymiar technologiczny i cyfrowy. Do zapewnienia sobie akceptowalnego poziomu autonomii w tym obszarze dążą państwa przykładające dużą wagę do swojej suwerenności, zarówno demokratyczne, jak i autorytarne. Istotność tej materii pokazały konflikty technologiczne i gospodarcze (w tym tzw. wojna o chipy pomiędzy USA i Chinami), jak również pandemia Covid-19 (przerwanie łańcuchów dostęp, znaczenie własnej produkcji sprzętu medycznego i leków) i związane z nią przyspieszenie cyfryzacji niemal wszystkich dziedzin życia społecznego. Także pełnoskalowa wojna Rosji z Ukrainą pokazała znaczenie nie tylko posiadania własnej bazy przemysłowej produkującej uzbrojenie i amunicję, ale również innych towarów i usług ważnych dla funkcjonowania państwa i społeczeństwa.

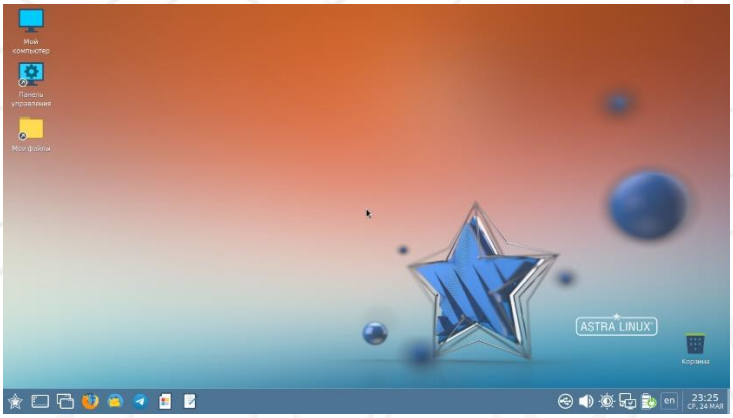
Z jednej strony, suwerenność cyfrowa rozumiana jako oddziaływanie państwa w wymiarze informacyjno-propagandowym oraz kontroli społeczeństwa i jego aktywności w sieci jest w większym stopniu domeną reżimów niedemokratycznych (choć nie tylko, wszak państwa demokratyczne też prowadzą aktywne działania informacyjne, dbają o swoją komunikację strategiczną, posiadają środki inwigilacji). Z drugiej strony istnieje też aspekt rozwiązań hardware'owych i software'owych mających realnie zapewnić suwerenność technologiczną. Jednym z państw, które aktywnie działa na tym polu jest Federacja Rosyjska, co w tym przypadku przekracza naturalną chęć uzyskania pewnej autonomii, a wynika z wrogiego postrzegania Zachodu, a więc i zachodnich rozwiązań technologicznych oraz chęci posiadania niezależności na wypadek odcięcia od zachodnich produktów i usług.

Koncepcja rosyjskiej suwerenności technologicznej/cyfrowej zawiera szereg kluczowych rozwiązań sprzętowych oraz w warstwie oprogramowania, wpływających na wzrost autonomii państwa oraz ograniczających możliwość wpływu państw trzecich w funkcjonowanie w „krajowego Internetu" (tzw. runet). Zaliczyć do nich należy:

- **SORM** (System Operacyjno-Poszukiwawczy Wydarzeń) - system nadzoru elektronicznego - umożliwia Federalnej Służbie Bezpieczeństwa (FSB) monitorowanie aktywności telefonicznej i internetowej obywateli. Program został uruchomiony w 1995 r., obecnie obejmuje również dostawców usług internetowych oraz firmy świadczące usługi cyfrowe. SORM działa poprzez instalację urządzeń monitorujących w sieciach telekomunikacyjnych, co pozwala na przechwytywanie wiadomości tekstowych, połączeń głosowych oraz ruchu internetowego.
- Próby władz FR **kontrolowania rosyjskich platform internetowych** powstałych jako alternatywy dla zachodnich odpowiedników, które są bardzo popularne na całym obszarze poradzieckim (np**. Yandex, Telegram, VKontakte**).
- Rodzinę **procesorów „Elburs"** wytwarzanych lokalnie, zaprojektowanych pod optymalne wykorzystanie **własnej dystrybucji systemów operacyjnych Linux** (**Astra Linux**) oraz **Aurora dla urządzeń mobilnych**, na wzór optymalizacji programowo-sprzętowej środowiska MacOS – perspektywicznie przeniesienie całego sektora publicznego na AstraLinux i stacje robocze oparte o Elbrus.

- Rodzina **procesorów graficznych „Bajkał”** – koncepcja analogiczna do ww. (ma to szczególne znaczenie w kontekście AI).
- **Rosyjskie narzędzia AI (np. GigaChat, Kandinsky 2.2).**
- **Rozwój własnych systemów płatności (np. MIR)**, co ma szczególne znaczenie w kontekście sankcji i odcięcia Rosji od systemu SWIFT.
- **Opracowywanie własnych smartfonów** (choć często na bazie chińskich komponentów).
- **Mechanizmy do rozwoju własnych technologii** (np. **technopolis Skołkowo** na potrzeby cywilne oraz **wojskowe innowacyjne technopolis ERA** na potrzeby obronne).

Rosyjski procesor Elbrus



Rosyjska dystrybucja systemu operacyjnego Linux - Astra

Powyższe inicjatywy napotykają wiele problemów, co wynika głównie z ograniczonych kompetencji technologicznych i przemysłowych, które dodatkowo są pogłębiane przez sankcje. Wpływ na to będzie też mieć exodus programistów i inżynierów zaobserwowany po 2022 r. Niemniej Federacja Rosyjska jest dosyć konsekwentna w realizacji swoich priorytetów.

Należy również wskazać, że Strategia Bezpieczeństwa Narodowego FR przyjęta w 2021 r. przewiduje szereg działań, które mają zwiększyć suwerenność Rosji w przestrzeni informacyjnej (pkt 57), w tym rozwój sił i środków walki w cyberprzestrzeni i walki informacyjnej, oraz szeroko rozumiane zwiększenie bezpieczeństwa systemów teleinformatycznych. Zapisy dotyczące suwerenności technologicznej znalazły się też w poprzedniej Strategii z 2015 r., jak również w innych dokumentach strategicznych i doktrynalnych.

Źródła: CNews.ru, wccftech.com, DFRLab.org, Pravo.gov.ru.

CBZC: Reagujemy na każde zgłoszenie dotyczące zagrożenia życia

Policjanci Centralnego Biura Zwalczania Cyberprzestępczości poza wykonywaniem zadań związanych ze zwalczaniem cyberprzestępczości, realizują również czynności w przypadku otrzymania informacji od podmiotów współpracujących z Biurem, z której wynika, że czyjeś życie jest zagrożone. Od początku wakacji funkcjonariusze podjęli działania w 341 przypadkach, z których aż 242 dotyczyło małoletnich.

Sekcja Obsługi Całodobowej Wydziału Wywiadu Kryminalnego, to jedna z komórek organizacyjnych Centralnego Biura Zwalczania Cyberprzestępczości, która realizuje czynności związane z ratowaniem życia ludzi, które znalazły się w trudnej sytuacji życiowej i są w kryzysie emocjonalnym. Działania podejmowane są na każde zgłoszenia otrzymane od partnerów współpracujących z Biurem, a które dotyczą informacji znalezionej w sieci Internet, z której wynika że ludzkie życie jest zagrożone.

Właściwa i szybka reakcja na takie zgłoszenie, daje szansę na udzielenie pomocy osobie, której wydaje się, że jest w sytuacji bez wyjścia. Policjanci nie lekceważą żadnego zgłoszenia, a każdy sygnał jest szczegółowo sprawdzany. Od początku roku funkcjonariusze podjęli już 1627 czynności ustaleniowych, z czego aż 1033 dotyczyło osób małoletnich. W 893 przypadkach działania zakończyły się umieszczeniem młodej osoby w szpitalu lub przekazaniem osobie najbliższej pod opiekę. Tylko od początku wakacji do 31 lipca policjanci CBZC, podjęli 341 czynności z czego 242 dotyczyło małoletnich. Wobec 195 konieczna była dalsza pomoc szpitalna lub opieka osoby najbliżej.

Pamiętajmy, że sytuacje kryzysowe są przemijające. Wielu tragedii można uniknąć, wzywając pomoc. Jeśli widzimy, że osoba z naszego otoczenia jest przygnębiona, zapytajmy, jak możemy jej pomóc. Jeśli dzieje się coś złego i wiemy, że życie oraz zdrowie tej osoby może być zagrożone, zadzwońmy pod numer alarmowy 112 i postarajmy się przekazać służbom lokalizację, w której znajduje się potrzebujący pomocy. W takich sytuacjach czas ma decydujące znaczenie.

Gdzie szukać pomocy?

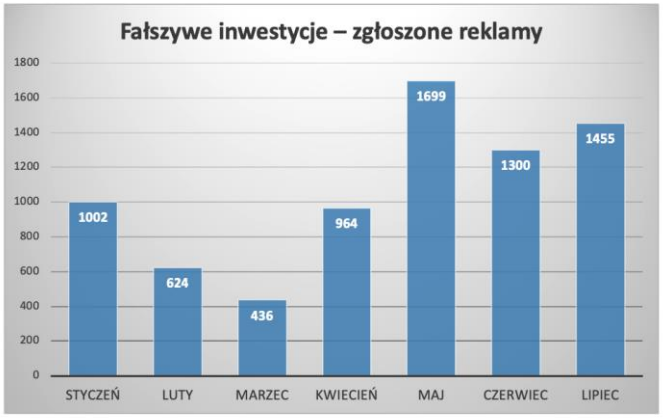
- 112 – numer alarmowy, który w stanach nagłego zagrożenia ratuje ludzkie życie.
- 800 70 2222 – całodobowy telefon Centrum Wsparcia dla osób w kryzysie psychicznym, depresji i z myślami samobójczymi, prowadzony przez Fundację ITAKA.
- 116 111 – całodobowy Telefon Zaufania dla Dzieci i Młodzieży, oraz 800 100 100 – telefon dla Rodziców i Nauczycieli w Sprawie Bezpieczeństwa Dzieci, prowadzony przez Fundację Dajemy Dzieciom Siłę (czynny od poniedziałku do piątku w godz. 12.00–15.00).
- 800 120 002 – całodobowy, bezpłatny telefon Ogólnopolskiego Pogotowia dla Ofiar Przemocy w Rodzinie „Niebieska linia”.
- Strony internetowe, np.: www.pokonackryzys.pl czy www.liniawsparcia.pl. Można za ich pośrednictwem porozmawiać przez czat internetowy lub uzyskać odpowiedzi na pytania drogą e-mailową.

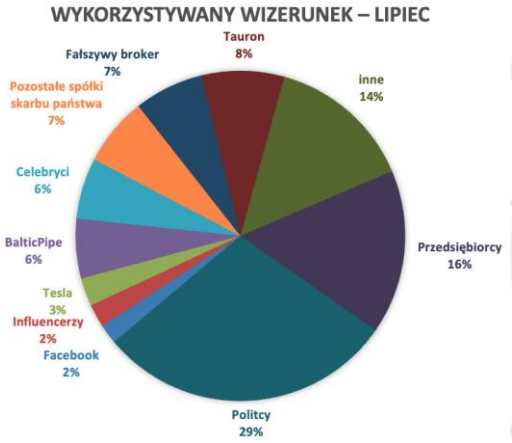
Więcej informacji: https://cbzc.policja.gov.pl/bzc/aktualnosci/378,Reagujemy-na-kazde-zgloszenie-dotyczace-zagrozenia-zycia.html

Cyberpodsumowanie miesiąca z perspektywy CSIRT KNF – Ochrona klienta

W lipcu 2024 roku CSIRT KNF wykrył i zgłosił do zablokowania 4 081 domeny, które wcześniej zakwalifikowane zostały jako wyłudzające dane (loginy i hasła do bankowości elektronicznej, informacje o kartach płatniczych, kody BLIK i/lub dane osobowe, etc.), dla porównania CERT Polska dodał na listę ostrzeżeń 7 919 domen. Na koniec omawianego miesiąca, na liście hole znajdowało się 217 309 domen.

Znanym, ale niezmiennie aktywnym scenariuszem przestępczym jest schemat znany pod nazwą „fałszywe inwestycje". Przestępcy dystrybuują go za pomocą reklam m.in. na platformie Facebook. Informują w nich o rzekomej możliwości inwestowania. CSIRT KNF wypracował mechanizmy wykrywające takie działanie przestępcze oraz procesy przekazywania fałszywych reklam do blokady. Poniższy wykres przedstawia wykryte i zgłoszone do blokady reklamy fałszywych inwestycji na portalu Facebook, w podziale na kategorie wykorzystywanego wizerunku.

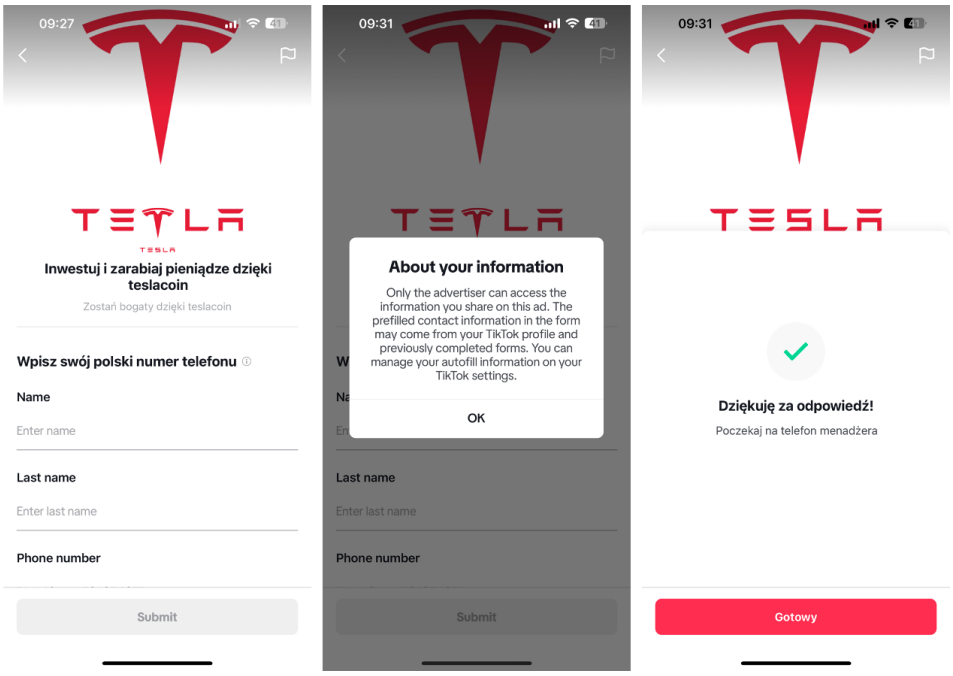




Dodatkowo, w lipcu 2024 roku analitycy CSIRT KNF ponownie wykryli i zgłosili do blokady 427 fałszywe profile (366 w czerwcu 2024), które publikowały fałszywe reklamy inwestycyjne. W lipcu 2024 roku CSIRT KNF wykrył również fałszywe reklamy inwestycyjne dystrybuowane poprzez platformę TikTok (rys. 1).

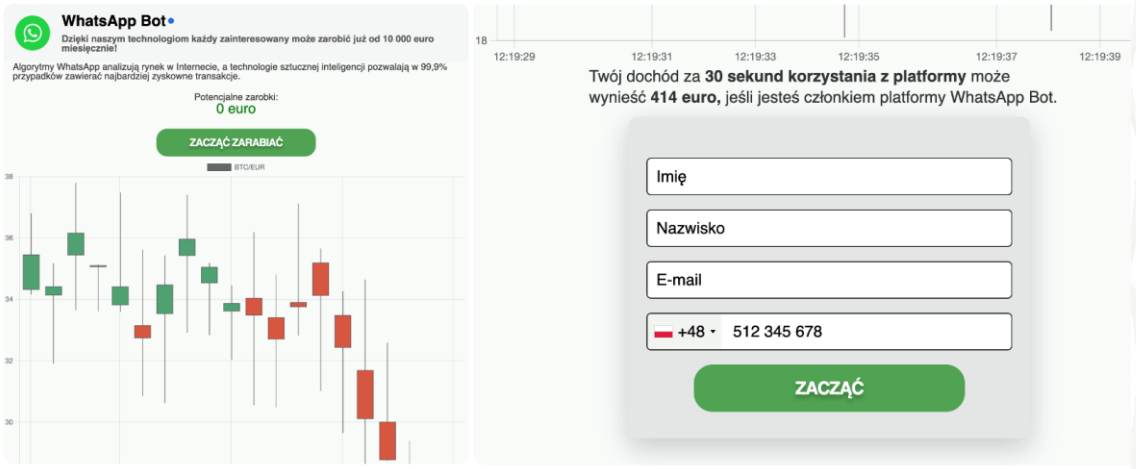
rys. 1 Fałszywe reklamy inwestycyjne dystrybuowane na platformie TikTok

Po kliknięciu w reklamę, ofiara trafia do formularza, gdzie wypełniała informacje dotyczące danych kontaktowych (rys. 2). W następnym etapie następuje kontakt telefoniczny.



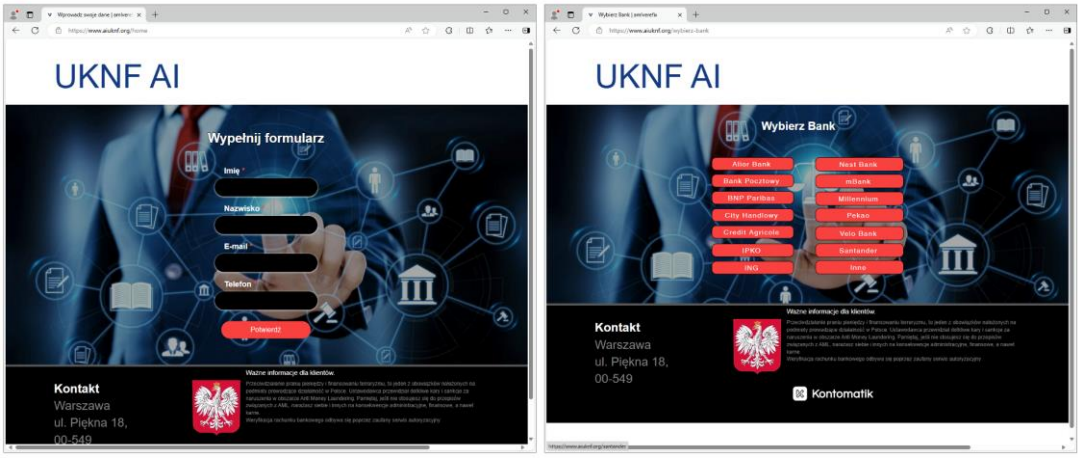
rys. 2 Fałszywe reklamy inwestycyjne - formularz na platformie TikTok

Podobnie jak w minionych miesiącach, atakujący przygotowali również aplikacje, mające na celu zachęcenie do rzekomego inwestowania. Aplikacje te są fałszywe, jednak nie infekują urządzeń. Mają na celu uwiarygodnianie scenariusza phishingowego (rys. 3).



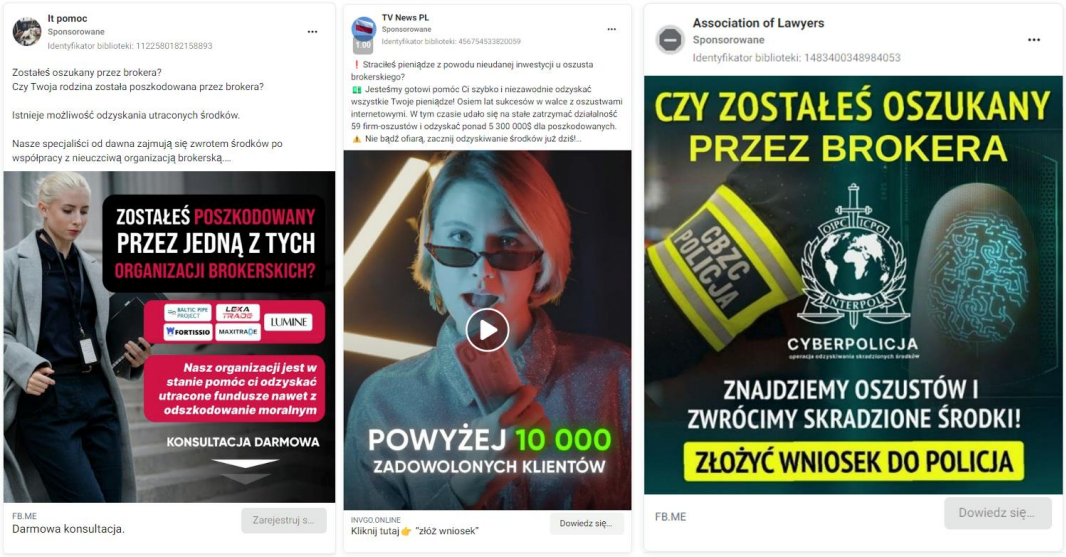
rys. 3 Oszukańcza aplikacja inwestycyjna

Zdarza się również, że innym sposobem na wzmocnienie prowadzanej gry psychologicznej, jest wykorzystanie wizerunku Urzędu Komisji Nadzoru Finansowego. W lipcu 2024 przestępcy ponownie przygotowali strony podszywające się pod UKNF. Ofiary informowali o rzekomej konieczności przejścia procesu „przeciwdziałania praniu pieniędzy". W tym celu wysyłali link do strony „UKNF AI", gdzie ofiara miała wpisać dane osobowe, wybrać bank i przekazać dane uwierzytelniające do bankowości elektronicznej (rys. 4).



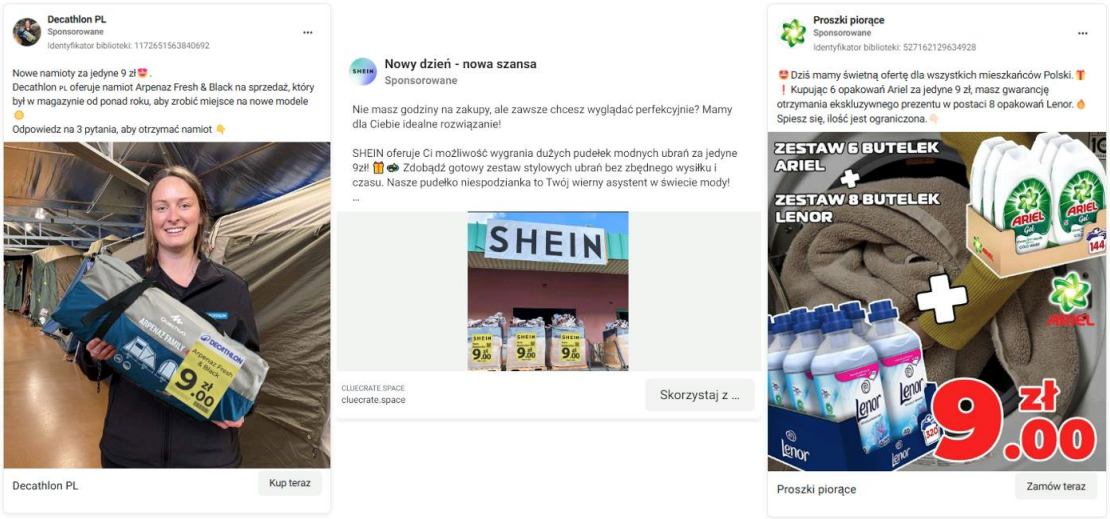
rys. 4 Fałszywe inwestycje - podszycie pod UKNF

Powtarzającym się schematem jest również drugi etap omawianego oszustwa. W nim, przestępcy publikują informację o rzekomej możliwości odzyskania utraconych wcześniej pieniędzy. W rzeczywistości, jest to ponowna próba oszukania osób, które już wcześniej dały się nabrać na ten scenariusz (rys. 5).



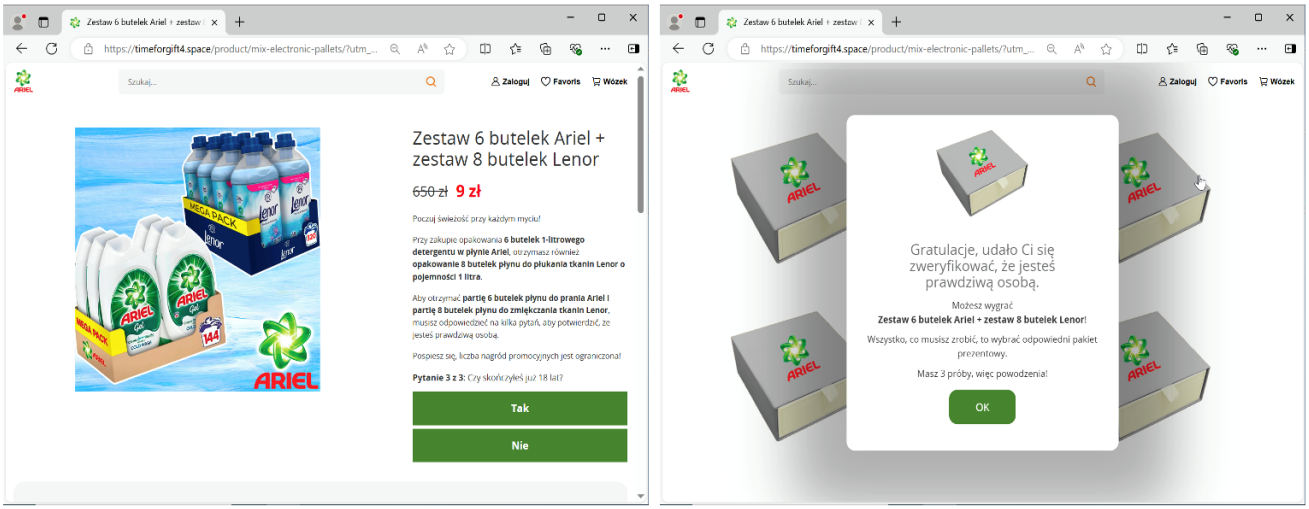
rys. 5 Fałszywe inwestycje - drugi etap oszustwa

W lipcu 2024 atakujący podszywali się pod również wizerunki polskich banków. Strony phishingowe dystrybuowali m.in. za pośrednictwem reklam na platformach społecznościowych, wiadomości e-mail oraz SMS. Stosując znane mechanizmy manipulacyjne zachęcali do kliknięcia w link, rzekomą możliwością odebrania nagrody lub zastraszali groźbą zablokowania bankowości elektronicznej. Tym sposobem starali się wyłudzać dane uwierzytelniające do bankowości elektronicznej oraz informacje o kartach płatniczych. Kolejnym schematem analizowanym w lipcu'24 były kampanie phishingowe wyłudzające dane kart płatniczych, pod pretekstem rzekomej możliwości nabycia różnych przedmiotów na jedyne 9zł (rys. 6).



rys. 6 Fałszywe reklamy - towar za 9zł

Jeżeli ktoś dał skusić się ofertą i kliknął w link, trafiła na stronę, na której proszony był o odpowiedź na kilka pytań (rys. 7). Następnie wyświetlał się formularz do wpisania danych osobowych oraz informacji o karcie płatniczej: numer karty, kod CVV, data ważności, kody 3DSecure.



rys. 7 Fałszywe reklamy – pytania „weryfikacyjne”

Jak co miesiąc mierzyliśmy się również ze znanymi od dawna schematami, takimi jak „scam na kupującego”, podszycia pod platformy streamingowe, wykorzystywanie wizerunku firma kurierskich, Poczty Polskiej i inne.

Przypominamy również, że aktualności o cyberzagrożeniach oraz trendach fraudowych publikujemy również na stronie internetowej UKNF oraz na profilach w mediach społecznościowych: X (Twitter), LinkedIn oraz Facebook do śledzenia których zachęcamy!

INFORMACJA O SZKOLENIACH

Zachęcamy również do udziału w bezpłatnych szkoleniach online dla podmiotów krajowego systemu cyberbezpieczeństwa, które organizuje Departament Cyberbezpieczeństwa MC.

Wszystkie informacje na temat szkoleń (w tym harmonogram i formularze zgłoszeń) znajdują się na stronie internetowej bazy wiedzy cyberbezpieczeństwa na portalu *gov.pl* – pod linkiem: https://www.gov.pl/web/baza-wiedzy/szkolenia

Zachęcamy również do zasubskrybowania biuletynu NASK – jest to przegląd najważniejszych informacji nt. cyberbezpieczeństwa, edukacji cyfrowej i nowych technologii.

Link do zapisów:

https://www.nask.pl/pl/aktualnosci/5166,Subskrybuj-Biuletyn-NASK-na-LinkedIn.html

Źródło: *nask.pl*

Oznaczenia TLP

Traffic Light Protocol (TLP) jest to zestaw reguł, pogrupowanych w 4 kategorie, używanych w celu lepszego zdefiniowania grupy odbiorców wrażliwych informacji. Dla ułatwienia kategorie opisywane są czterema kolorami (czerwony, pomarańczowy, zielony oraz biały). Zakwalifikowanie do odpowiedniej kategorii leży po stronie organizacji, z której pochodzą informacje. Jeśli odbiorca chciałby podzielić się uzyskanymi informacjami z szerszym gronem, musi uzyskać odpowiednią akceptację od autora wiadomości.

Oznaczenie	Odbiorca wiadomości	Autor wiadomości
TLP:RED	Odbiorcy nie mogą dzielić się przekazanymi informacjami z nikim, z wyjątkiem innych odbiorców tych wiadomości.	Oznaczenie wiadomości, które mogą za sobą nieść poważne zagrożenie ujawnienia wrażliwych danych w wyniku ich nieprawidłowego przetworzenia, jak również, gdy ich wykorzystanie przez innych niż odbiorcy nie ma sensu.
TLP:AMBER	Odbiorcy mogą dzielić się informacjami jedynie w obrębie swojej organizacji (a także jej klientów i consituency) z osobami, które muszą poznać wiadomości oraz jedynie w zakresie niezbędnym do podjęcia stosownych działań. Dodatkowe ograniczenia mogą zostać wyspecyfikowane przez nadawcę w dowolnym zakresie i muszą być przestrzegane. Jednym ze standardowych ograniczeń jest oznaczenie TLP:AMBER+STRICT **, które pozwala dzielić się informacjami wyłącznie w obrębie organizacji.**	Oznaczenie wiadomości wymagających podjęcia odpowiednich kroków przez dodatkowe osoby. Informacje te niosą ze sobą ryzyko ujawnienia zbyt wielu wrażliwych danych, jeśli zostałyby przekazane podmiotom innym niż bezpośrednio zaangażowanym.
TLP:GREEN	Odbiorcy mogą dzielić się informacji ze swoimi współpracownikami, w ramach swojej i partnerskich organizacji oraz w swoim środowisku. Nie można jednak udostępniać tych informacji przez publiczne kanały informacyjne.	Oznaczenie wiadomości niosących ze sobą informacje ogólnie przydatne dla wszystkich organizacji partnerskich oraz w obrębie środowiska.
TLP:CLEAR	Dystrybucja informacji nie podlega żadnym ograniczeniom (z wyjątkiem praw autorskich).	Oznaczenie wiadomości, których wykorzystanie nie powinno wiązać się z żadnym bądź minimalnym ryzykiem niewłaściwego użycia.

Źródło: *cert.pl*

Biuletyn został opracowany przez Wydział Analiz Cyberbezpieczeństwa Departamentu Cyberbezpieczeństwa Ministerstwa Cyfryzacji we współpracy z zespołami CSIRT KNF i CBZC.