Ministerstwo Cyfryzacji

Departament Cyberbezpieczeństwa

TLP:GREEN

BIULETYN INFORMACYJNY

ZAGROŻENIA W CYBERPRZESTRZENI

06/2025

SPIS TREŚCI

Doktryna CyberPiastowska

Premier polskiego rządu z okazji 1000-lecia koronacji Bolesława Chrobrego ogłosił Doktrynę Piastowską. Jej trzema filarami mają być (I) najsilniejsza w regionie armia, (II) najsilniejsza gospodarka w regionie oraz (III) pozycja polityczna w regionie i w Europie. W ramach działań z zakresu ekonomii kluczowe mają być deregulacja oraz repolonizacja gospodarki. W celu wsparcia rodzimych przedsiębiorstw mają one być – w ramach obowiązującego prawa– faworyzowane w przetargach przy zamówieniach publicznych.

Choć doktryna ta nie ma podstaw w dokumentach strategicznych i doktrynalnych Państwa Polskiego, warto spojrzeć jak mogłaby się ona zmaterializować w obszarze cyberbezpieczeństwa. Bowiem wojny handlowe i technologiczne, narastająca rywalizacja mocarstw oraz destabilizacja ładu międzynarodowego, sprawiają, że posiadanie własnej silnej bazy przemysłowo-technologicznej jest kluczowe dla bezpieczeństwa narodowego i rozwoju gospodarczego.

Uroczyste Zgromadzenie Posłów i Senatorów z okazji 1000-lecia koronacji Bolesława Chrobrego. Źródło: KPRM

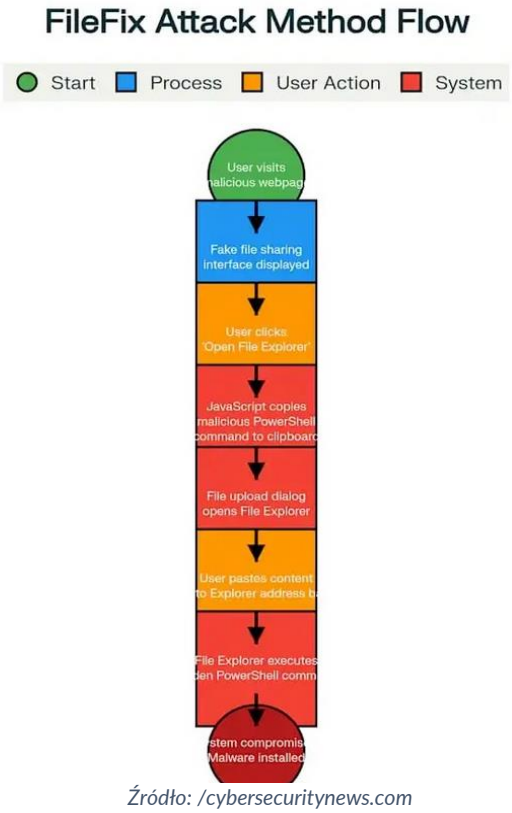
Aby osiągnąć rezultaty w tym zakresie **instytucje publiczne**, w ramach dopuszczonych prawem formach, w tym przy poszanowaniu reguł rynku wewnętrznego UE, mogłyby **ukierunkowywać swoje działania, aby korzystać przede wszystkim z rozwiązań cyberbezpieczeństwa rodzimych polskich firm**, w przypadku gdy są one konkurencyjne i spełniają wymagania zamawiającego. Pozwoliłoby to zbudować w Polsce silne marki i sektor cyberbezpieczeństwa oraz wspierałoby ekspansję zagraniczną polskich przedsiębiorstw z branży cyberbezpieczeństwa, a także przełożyłoby się na wzmocnienie suwerenności państwa w zakresie technologii oraz strategicznej autonomii decyzyjnej. Przyczyniłoby się to także do uniezależnienia od wielkich zagranicznych korporacji technologicznych.

Jednak, aby polskie firmy oferowały konkurencyjne, nowoczesne i innowacyjne produkty konieczne zapewnienie przez państwo optymalnych warunków do prowadzenia działalności gospodarczej (w tym poprzez deregulację) oraz ambitne nakłady publiczne na badania i rozwój na rzecz polskich podmiotów. Pozwoli to prowadzić prace nad stworzeniem polskich rozwiązań cyberbezpieczeństwa, zarówno sprzętowych, jak i programowych. Krajowy potencjał przemysłu cyberbezpieczeństwa mógłby dzięki temu zapewnić suwerenne zdolności m.in. w zakresie tworzenia mikroprocesorów i innego rodzaju układów scalonych, modułów pamięci, mikrokontrolerów, układów kryptograficznych, programowalnych urządzeń sieciowych oraz algorytmów uczenia maszynowego.

Źródła: *KPRM, MC.*

FileFix nowa wersja ataku ClickFix

W ostatnim czasie pojawiła się ulepszona wersja ataku socjotechnicznego ClikFix, pod nazwą FileFix. Technika ClickFix polegała na nakłonieniu użytkownika do nieświadomego wykonania złośliwego polecenia systemowego, zwykle poprzez okno dialogowe Uruchom (skrót Windows + R). Atakujący tworzył instrukcję, w której prosił ofiarę o skopiowanie ciągu znaków, wyglądający na niewinną komendę, a w rzeczywistości ukrywał tak polecenie PowerShell wywołujące złośliwe działanie. Mimo swej prostoty metoda okazywała się skuteczna, jednak jej głównym ograniczeniem było uzależnienie od ona dialogowego Mechanizm ataku FileFix opiera się na sprytnym wykorzystaniu funkcji przeglądarki i naiwności użytkownika. Gdy ofiara odwiedza przygotowaną stronę phishingową, widzi pozornie niewinną instrukcję dotyczącą otwarcia udostępnionego dokumentu. Strona zawiera przycisk "Otwórz Eksplorator Plików", który w rzeczywistości uruchamia standardowe okno wyboru pliku poprzez element input type file. Kluczowy moment następuje, gdy użytkownik próbuje skopiować i wkleić podaną "ścieżkę do pliku". W rzeczywistości otrzymuje on starannie przygotowany ciąg znaków *„Powershell.exe -c ping example.com # C:\\company\\internal-secure\\filedrive\\HRPolicy.docx”* Ścieżka na pierwszy rzut oka wygląda niewinnie, jednak kod przedzielony jest znakiem „#” i ukryty w dalszej części wiersza, w ten właśnie sposób zamiast wejść do katalogu, uruchamiana jest komenda PowerShell, wykonująca np. połączenie sieciowe, pobranie malware lub inną złośliwą operację. Możliwy jest również wariant z plikiem exe, który jest pobierany i uruchamiany w podobny sposób, co ważne uruchomienie pliku przez pasek adresu Eksploratora usuwa tzw. Mark of The Web (MOTW), czyli atrybut wskazujący, że plik pochodzi z internetu, co może ułatwić ominięcie niektórych zabezpieczeń systemu. Kolejny wariant ataku oparty jest na plikach .hta. Strona phishingowa proponuje ofierze zapisanie pliku w formacie hta, następnie uruchamiany jest mshta.exe, który wykonuje złośliwy kod.



Źródło: /cybersecuritynews.com

FileFix różni się od tradycyjnego phishingu tym, że nie polega na podszywaniu się pod strony logowania ani na wyłudzaniu danych. Nie chodzi tu o zdobycie haseł czy tokenów, lecz o nakłonienie użytkownika do uruchomienia polecenia, które daje atakującemu zdalny dostęp lub pozwala pobrać kolejne złośliwe oprogramowanie. To subtelna, ale bardzo groźna ewolucja phishingu, bo przekracza granicę między socjotechniką a wykorzystaniem mechanizmów systemu operacyjnego.

Źródła: *mrd0x.com, cybersecuritynews.com,*

Grupa BERT – nowe zagrożenie w krajobrazie ransomware 2025

W kwietniu br. badacze z firmy TrendMicro (TM) wykryli i zdefiniowali nową grupę ransomware o globalnym zasięgu – BERT, kod nazwowy TM: Water Pombero. Ugrupowanie nie zostało jeszcze oficjalnie zarejestrowane jako osobny podmiot w bazie MITRE ATT&CK. Grupa wpisuje się w rosnący trend zagrożeń w dynamicznym krajobrazie cyberprzestępczości. Należy zwrócić uwagę, że BERT wyróżnia się zdolnością prowadzenia ataków zarówno na systemy operacyjne Windows, jak i Linux, co świadczy o szerokim wachlarzu zdolności aktywnych. Analiza powłamaniowa TM dowodzi, że grupa celuje w krytyczne sektory gospodarki państw z różnych zakątków świata.

Źródło: fortra.com

Aktywność grupy wpisuje się w globalny trend na „rynku ransomware". Zgodnie z danymi opublikowanymi przez izraelską firmę CheckPoint w 2025 r. obserwujemy rekordowy wzrost aktywności ransomware na świecie. W pierwszym kwartale br. liczba ataków wzrosła o 126% w porównaniu rdr.

Należy pamiętać, że firmy komercyjne zajmujące się cyberbezpieczeństwem tworzą swoje raporty na danych pochodzących z własnych systemów monitoringu, jak końcówki (endpointy) oraz sond instalowanych w zabezpieczanych systemach IT. Zakres danych jest ograniczony do obsługiwanej infrastruktury, jednakże sama skala obserwowanego wzrostu złośliwej aktywności grup APT w br. jest zauważalna, potwierdzona przez wielu różnych dostawców rozwiązań bezpieczeństwa i wpisuje się w globalne trendy.

Zgodnie z ogólnie dostępnymi analizami można stwierdzić, iż BERT wykorzystuje infrastrukturę powiązaną z ASN 39134[1] zarejestrowanym w Rosji (FR). Powyższe może wskazywać na powiązania grupy z regionem wschodnioeuropejskim/zachodnioazjatyckim. Charakterystyczne jest żądanie okupu w kryptowalucie Monero oraz komunikacja poprzez zaszyfrowane kanały w sieci Tor. Na chwilę obecną brak jest informacji dot. profilu ideologicznego BERT oraz motywacji innych niż finansowe, co uniemożliwia sprofilowanie grupy jako związanej z aparatem państwowym FR. Jednakże dobór geograficzny celów (Azja, Europa, Ameryka Północna), jest spójny z modus operandi rosyjskich służb specjalnych, które dają ciche przyzwolenie organizacjom przestępczym na prowadzenie złośliwej działalności internetowej wobec podmiotów znajdujących się w państwach nieprzychylnych FR.

Źródło:trendmicro.com

[1] ASN, czyli Autonomous System Number (Numer Systemu Autonomicznego), to unikalny identyfikator przypisany do systemu autonomicznego w Internecie. System autonomiczny to zbiór adresów IP zarządzanych przez jedną organizację (np. dostawcę internetu, dużą firmę, operatora chmury), który stosuje spójną politykę routingu.

Sytuacja w Polsce

Według badaczy z firmy ESET, w pierwszej połowie br. Polska zajmuje pierwsze miejsce na świecie pod względem wykrytych ataków ransomware, odpowiadając za 6% globalnych incydentów. *wyprzedzając nawet Stany Zjednoczone.*

Przyczyną wysokiej pozycji są zarówno czynniki techniczne, jak i organizacyjne. Polska znajduje się wysoko w rankingach wykryć ransomware nie tylko z powodu zagrożeń zewnętrznych, ale również przez własne słabości.

Ponad jedna trzecia firm w kraju nie korzysta z podstawowego oprogramowania zabezpieczającego, a aż 88% organizacji padło ofiarą cyberataku lub wycieku danych w ostatnich latach. Problem pogłębia brak świadomości – tylko 19% pracowników wie, czym jest ransomware, a ponad połowa nie przeszła żadnego szkolenia z cyberbezpieczeństwa w ciągu ostatnich pięciu lat.

Natomiast według raportu *Microsoft Digital Defense Report*, Polska zajmuje 3. miejsce w Europie i 9. na świecie pod względem narażenia na ataki ze strony grup wspieranych przez obce państwa – głównie Rosję. Raport ujawnia również skalę zagrożeń i rosnącą rolę sztucznej inteligencji w ich odpieraniu:

- Microsoft (MS) analizuje już 78 bilionów sygnałów dziennie z chmury, urządzeń i partnerów (wzrost z 65 bln).
- Codziennie dochodzi do ponad 600 milionów prób ataków – od phishingu po ransomware.
- MS monitoruje ponad 1500 grup cyberprzestępczych, w tym 600 wspieranych przez państwa.

Podsumowanie

Dane te pokazują, że Polska znajduje się w centrum globalnej mapy zagrożeń cyfrowych i wymaga kontynuowania oraz intensyfikacji działań w zakresie zwiększania poziomu cyberochrony – zarówno na poziomie instytucjonalnym, jak i indywidualnym.

Globalny krajobraz ransomware w 2025 roku wyraźnie wskazuje na wzrost aktywności grup APT, mimo obserwowanego spadku wskaźników płatności okupu. To oznacza, że motywacje atakujących stają się coraz bardziej złożone – nie zawsze ograniczają się do zysku finansowego, ale mogą obejmować również cele polityczne, destabilizacyjne czy wywiadowcze.

W tym kontekście organizacje – zarówno publiczne, jak i prywatne – muszą przygotować się na coraz bardziej wyrafinowane i ukierunkowane ataki, szczególnie w środowiskach hybrydowych oraz w obszarze infrastruktury krytycznej. Kluczowe będzie nie tylko wdrażanie nowoczesnych technologii ochronnych, ale także budowanie świadomości zagrożeń, rozwój kompetencji kadry oraz współpraca międzynarodowa w zakresie wymiany informacji i reagowania na incydenty.

W obliczu takich wyzwań, cyberbezpieczeństwo przestaje być domeną wyłącznie działów IT – staje się strategicznym priorytetem dla całego państwa i każdej organizacji.

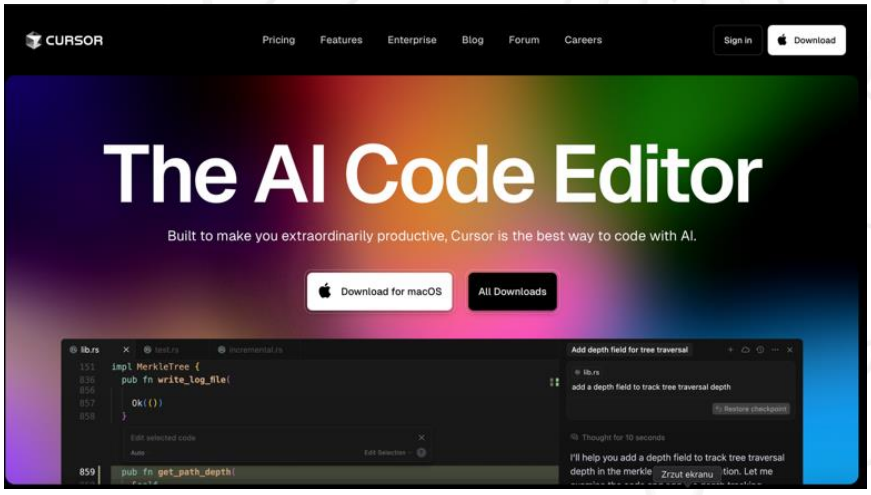
Vibe coding – przyszłość programowania czy tylko chwilowy hype? Analiza i szybki Proof of Concept na przykładzie aplikacji dla Ministerstwa Cyfryzacji

Vibe coding to nowe podejście do tworzenia oprogramowania, które wykorzystuje duże modele językowe (LLM) i podpowiedzi w języku naturalnym do generowania kodu. Podkreśla ono podejście oparte na współpracy i konwersacji między programistą a sztuczną inteligencją, pozwalając programistom skupić się na ogólnej wizji i funkcjonalności oprogramowania, podczas gdy sztuczna inteligencja zajmuje się technicznymi szczegółami implementacji. Metoda ta ma na celu uczynienie tworzenia oprogramowania bardziej dostępnym i potencjalnie szybszym, szczególnie w przypadku prostszych projektów lub prototypów.

Jak działa vibe coding w praktyce?

Vibe coding zazwyczaj obejmuje następujące kroki i odbywa się w powtarzającym się cyklu. Poniżej opracowany i opisany przez firmę Google proces vibe coding'u.

- **Wprowadzanie danych w języku naturalnym:** użytkownik dostarcza opis pożądanej funkcjonalności lub zadania w prostym języku (tekst lub głos) do asystenta kodowania AI. Te dane wejściowe służą jako punkt wyjścia.
- **Interpretacja AI:** Model AI analizuje dane wejściowe, identyfikuje kluczowe wymagania i określa niezbędną strukturę kodu i logikę.
- **Generowanie kodu:** W oparciu o swoją interpretację sztuczna inteligencja generuje kod, który może obejmować funkcje, klasy lub całe programy.
- **Wykonanie i obserwacja:** Użytkownik uruchamia wygenerowany kod, aby sprawdzić, czy działa on zgodnie z zamierzeniami.
- **Informacje zwrotne i udoskonalanie:** Jeśli wystąpią błędy lub funkcjonalność nie jest do końca poprawna, użytkownik przekazuje sztucznej inteligencji informacje zwrotne, często opisując problem w sposób naturalny (na przykład: „Zawiesza się, gdy wprowadzam liczbę ujemną") lub wklejając komunikaty o błędach. Następnie sztuczna inteligencja próbuje wygenerować poprawiony lub udoskonalony kod.
- **Powtarzanie:** Ten cykl generowania -> wykonywania -> obserwacji -> informacji zwrotnej -> poprawiania powtarza się, aż użytkownik osiągnie pożądany rezultat.



Źródło:cursor.com

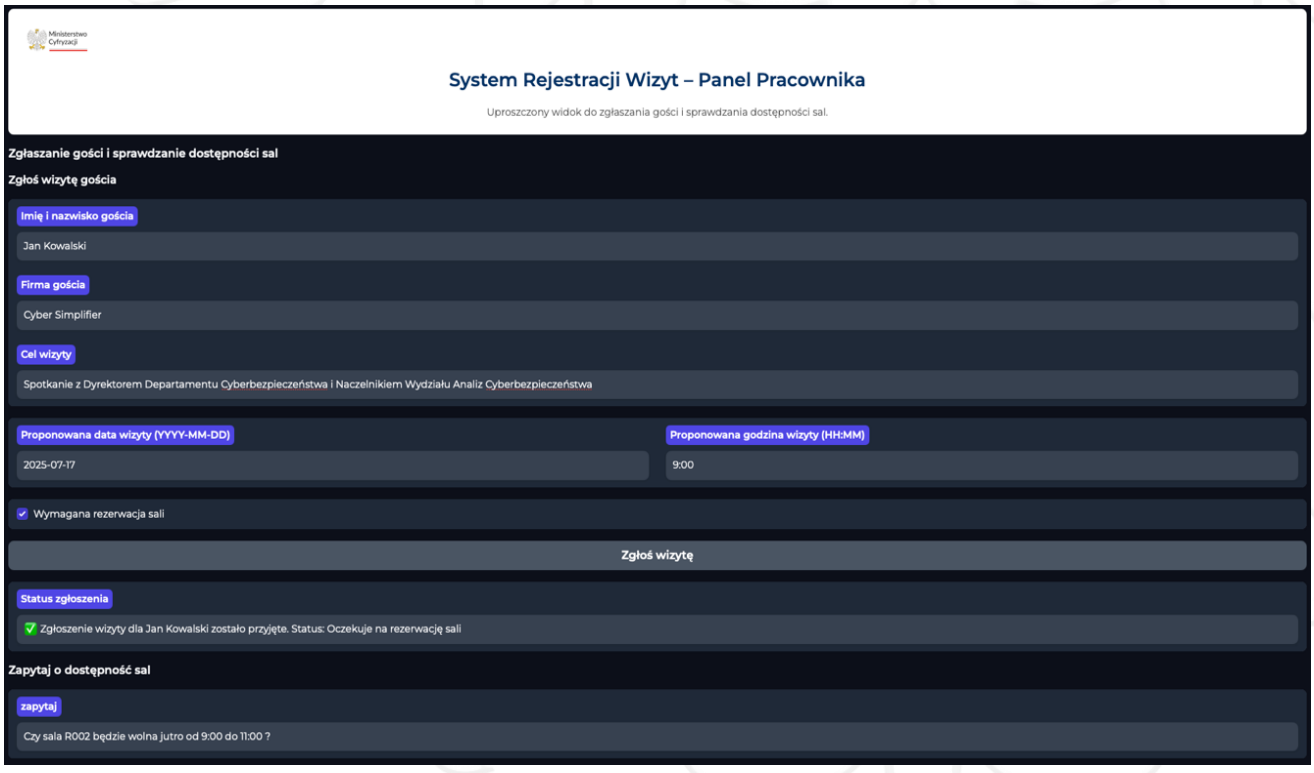
Poniżej Proof of Concept na przykładzie projektu interfejsu aplikacji do zarządzania wizytami gości (w tym zgłaszaniu), dostępnością i rezerwacją sal z modułem raportowania stworzony na potrzeby artykułu (bez ręcznego kodowania). Aplikacja posiada panel do logowania i podział na 2 role, pracownik oraz recepcja. Projekt zakłada możliwość sprawdzenia dostępności sal oraz wygenerowanie raportu statystyk dot. odwiedzających gości.

W projekcie wykorzystano m.in.:

- Google Colab (https://colab.research.google.com/)– Google Colab to środowisko notatników Jupyter hostowane w chmurze, które umożliwia pisanie i wykonywanie kodu Python w przeglądarce, bez konieczności konfiguracji. Zapewnia darmowy dostęp do procesorów graficznych i TPU, co jest przydatne do uczenia maszynowego i analizy danych. Narzędzie darmowe w dużym stopniu i niewymagające konfiguracji środowiska, jedynie zalogowania na koncie Google. Projekty zapisywane są bezpośrednio na dysku Google. A w nim:

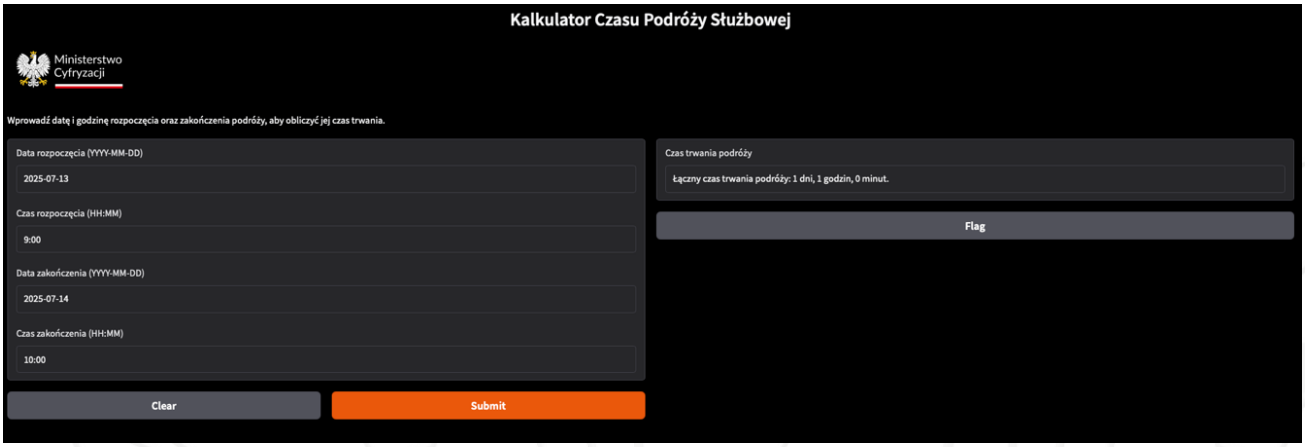
- *Framework webowy Gradio - biblioteka Python, która pozwala szybko tworzyć interfejsy użytkownika dla modeli uczenia maszynowego i funkcji Pythona. Upraszcza proces demonstracji modeli lub udostępniania aplikacji bez konieczności budowania pełnej aplikacji internetowej.*
- *Pandas (biblioteka do analizy i manipulacji danymi), os (moduł biblioteki Python do interakcji z system operacyjnym), datetime (moduł do pracy z datami i godzinami).*

Stworzenie projektu działającej aplikacji zajęło kilkanaście minut i oparte było głównie o wykorzystanie rozwiązania Google Colab i wymyślenie logiki działania aplikacji z ewentualnymi drobnymi korektami. Oczywiście wdrożenie takiej aplikacji w środowisku produkcyjnym wymagałoby znacznie więcej pracy niż tylko wygenerowanie kodu, jednak dzięki zastosowaniu takich rozwiązań można uzyskać bardzo dobrą bazę wejściową do wdrożenia faktycznie działającego rozwiązania.



Źródło: opracowanie własne, z wykorzystaniem rozwiązania Google Colab

Poniżej z kolei przykład prostej aplikacji do obliczania czasu trwania podróży służbowej.



Źródło: opracowanie własne, z wykorzystaniem rozwiązania Google Colab

```
## Frontend Security

| | Security Measure | Description |
|---|-----------------|-------------|
| □ | Use HTTPS everywhere | Prevents basic eavesdropping and man-in-the-middle attacks |
| □ | Input validation and sanitization | Prevents XSS attacks by validating all user inputs |
| □ | Don't store sensitive data in the browser | No secrets in localStorage or client-side code |
| □ | CSRF protection | Implement anti-CSRF tokens for forms and state-changing requests |
| □ | Never expose API keys in frontend | API credentials should always remain server-side |

## Backend Security

| | Security Measure | Description |
|---|-----------------|-------------|
| □ | Authentication fundamentals | Use established libraries, proper password storage (hashing+salting) |
| □ | Authorization checks | Always verify permissions before performing actions |
| □ | API endpoint protection | Implement proper authentication for every API endpoint |
| □ | SQL injection prevention | Use parameterized queries or ORMs, never raw SQL with user input |
| □ | Basic security headers | Implement X-Frame-Options, X-Content-Type-Options, and HSTS |
| □ | DDoS protection | Use a CDN or cloud service with built-in DDoS mitigation capabilities |

## Practical Security Habits

| | Security Measure | Description |
|---|-----------------|-------------|
| □ | Keep dependencies updated | Most vulnerabilities come from outdated libraries |
| □ | Proper error handling | Don't expose sensitive details in error messages |
| □ | Secure cookies | Set HttpOnly, Secure and SameSite attributes |
| □ | File upload security | Validate file types, sizes, and scan for malicious content |
| □ | Rate limiting | Implement on all API endpoints, especially authentication-related ones |
```

Źródło: gist.githubusercontent.com

Korzystając z metody vibe codingu zwłaszcza w przypadku mniej doświadczonych osób, warto pamiętać przede wszystkim o aspektach **bezpieczeństwa projektowanej aplikacji.**

Vibe coding to fascynujący trend, który może przekształcić sposób, w jaki powstają prototypy, narzędzia i MVP (Minimum Viable Product) - zwłaszcza w małych zespołach i krótkich, mniej skomplikowanych projektach. Jednak bez umiejętnego nadzoru, głębszego zrozumienia i standardów jakości może prowadzić do poważnych luk w bezpieczeństwie i trudnych do utrzymania rozwiązań. **Idealnie jest wykorzystać vibe coding tam, gdzie daje wartość, ale pamiętając o roli człowieka-programisty, który weryfikuje i dba o solidność kodu. Czy vibe coding zmieni świat IT? Być może. Ale nawet jeśli nie zastąpi tradycyjnego programowania, na pewno zmieni sposób, w jaki patrzymy na tworzenie oprogramowania.**

Efektywna praca policjantów CBZC – rozbicie grupy przestępczej i zatrzymanie 7 osób

Policjanci Zarządu w Poznaniu Centralnego Biura Zwalczania Cyberprzestępczości rozbili zorganizowaną grupę przestępczą, której członkowie wyłudzali pieniądze poprzez pozyskiwanie kodów BLIK. Oszukali w ten sposób ok. 1300 osób na ponad 3 mln złotych!

Przestępcy przy użyciu fałszywych kont wystawiali ogłoszenia do sprzedaży fikcyjnych przedmiotów, m.in. elektroniki. Następnym krokiem było wyłudzenie kodu BLIK od potencjalnego kupca. Docelowo oszuści transferowali uzyskane pieniądze na portfele kryptowalutowe. Policjanci zatrzymali 7 mężczyzn w wieku od 19 do 37 lat. Każda z osób usłyszała od 20 do ok. 370 zarzutów! Były to zarzuty udziału w zorganizowanej grupie przestępczej i odpowiednio kierowania grupą przestępczą oraz zarzuty prania pieniędzy i licznych oszustw, za co grozi kara do 15 lat pozbawienia wolności. Wobec wszystkich zatrzymanych sąd zastosował środek zapobiegawczy w postaci tymczasowego aresztowania na okres 3 miesięcy.

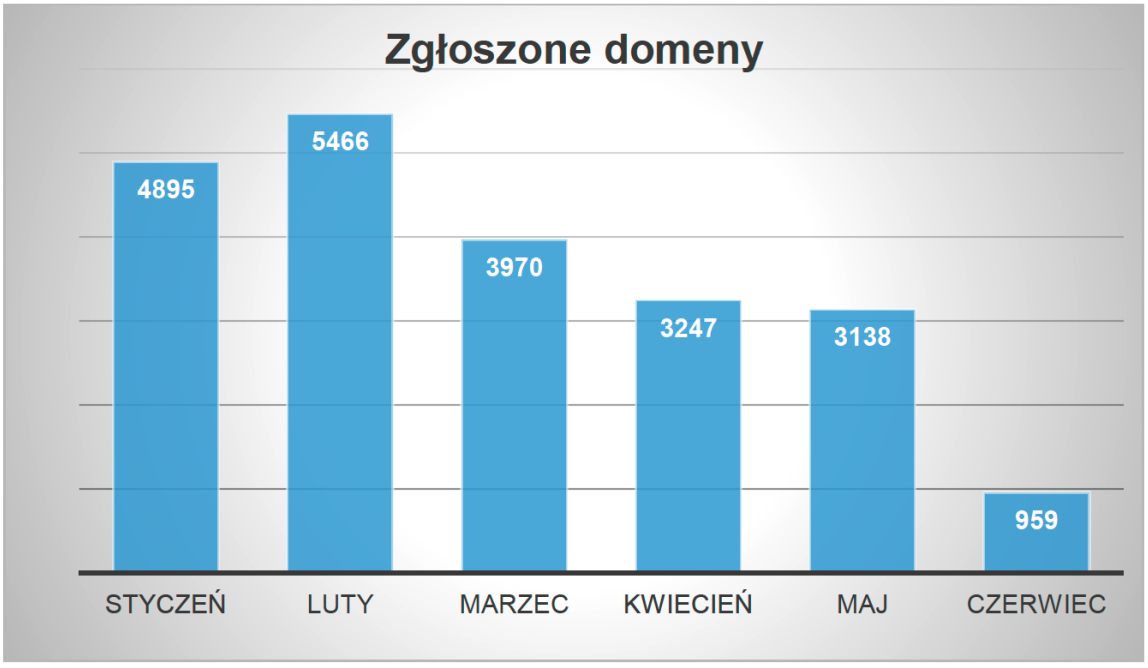
Działania realizowane były na terenie 5 województw: dolnośląskiego, mazowieckiego, warmińsko-mazurskiego, łódzkiego oraz podkarpackiego przy wsparciu Zarządu w Łodzi, w Rzeszowie oraz Zarządu we Wrocławiu CBZC. Podczas przeszukań pomieszczeń mieszkalnych funkcjonariusze zabezpieczyli różnego rodzaju nośniki danych – komputery, telefony i dyski. Wyliczenia strat są początkowe – sprawa jest rozwojowa, dlatego straty mogą być większe i niewykluczone są kolejne zatrzymania.

Sprawę nadzoruje Prokuratura Regionalna w Łodzi. Była to druga realizacja w tej sprawie. Do tej pory łącznie aresztowano 9 osób.

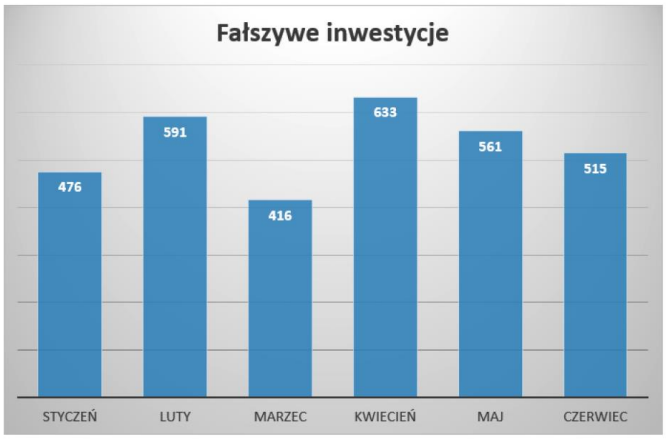
Źródło: CBZC

Podsumowanie miesiąca z przez CSIRT KNF

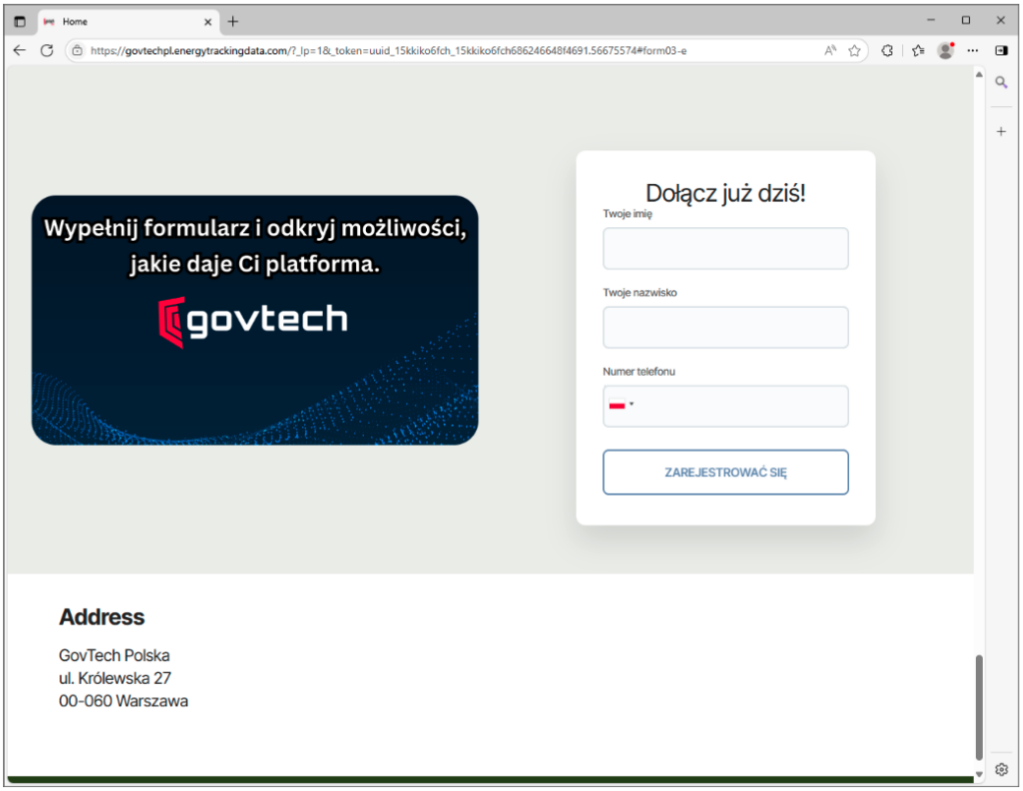
W czerwcu 2025 roku Zespół CSIRT KNF zgłosił do zablokowania 959 domen wykorzystywanych do wyłudzania danych. W pierwszym półroczu obecnego roku, działania CSIRT KNF skoncentrowane m.in na wykrywaniu i raportowaniu zagrożeń związanych z phishingiem, fałszywymi reklamami i aplikacjami mobilnymi, doprowadziły do wykrycia ponad 20 tys. stron wykorzystywanych przez przestępców.



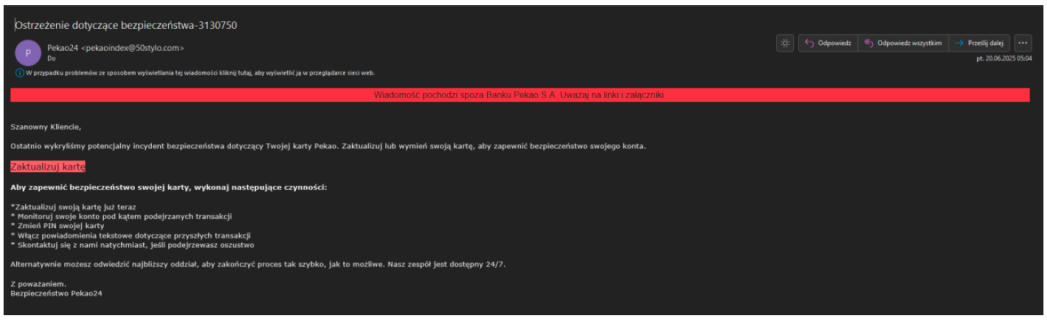
CSIRT KNF wykrył również 196 fałszywych profili na Facebooku, które promowały reklamy w kampanii znanej pod nazwą fałszywe inwestycje. Łącznie tego typu reklam, w czerwcu 2025 roku CSIRT KNF zgłosił do zablokowania 515.



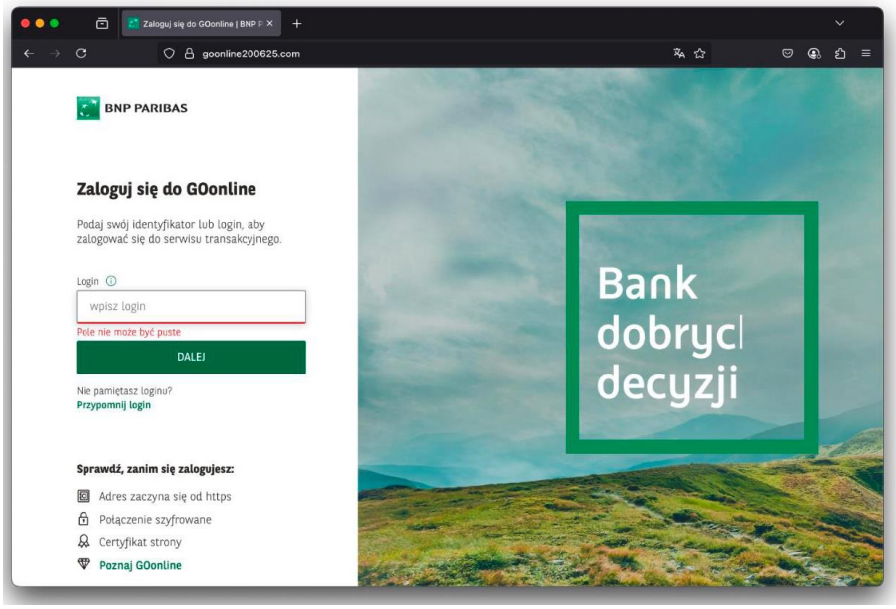
Ataki te bazują na kampaniach z wykorzystaniem formularzy rejestracyjnych i późniejszym kontakcie telefonicznym przestępcy z ofiarą, mającym na celu nakłonienie do przelewania wysokich kwot pieniędzy.



W czerwcu szczególną uwagę zwróciły kampanie phishingowe podszywające się bezpośrednio pod banki (PKO BP, Bank Pekao, BNP Paribas, Bank SGB). Oszuści wykorzystywali wiadomości e-mail, kierujące do stron podszywających się pod logowanie do bankowości elektronicznej.



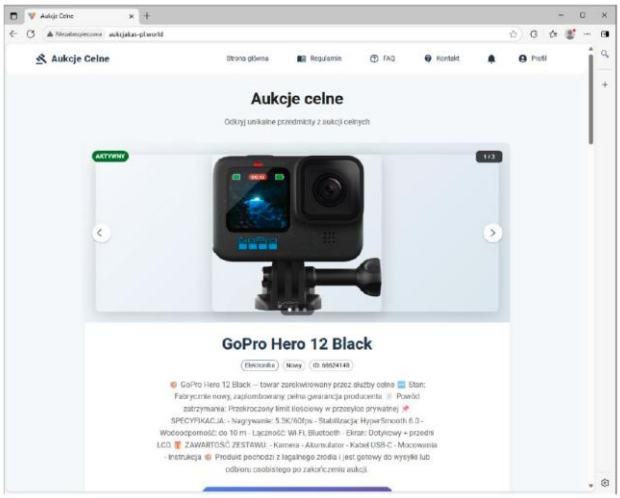
Celem było przejęcie poświadczeń i kodów dostępowych



Kreatywnością wykazały się również kampanie podszywające się pod popularne marki i instytucje publiczne. Fałszywe reklamy dotyczyły m.in.:

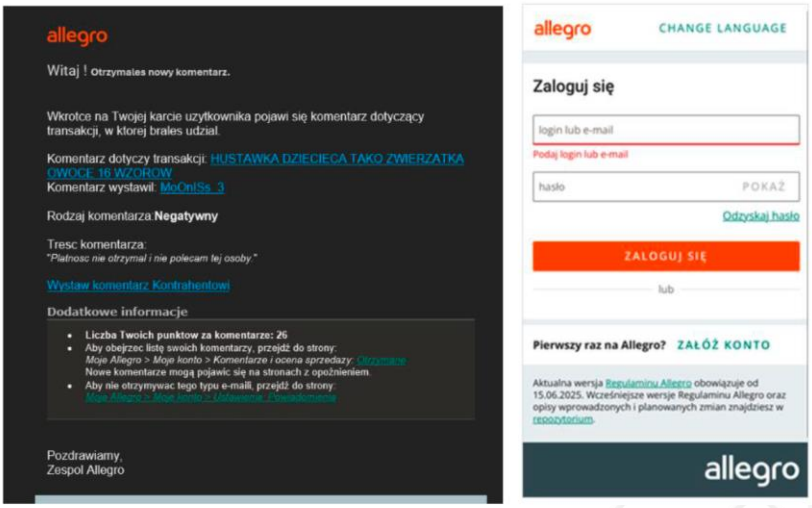
- kart miejskich,

- aukcji celnych (podszycie pod KAS),



- platform streamingowych (Spotify, Netflix, Disney+),

- portali zakupowych (Allegro).



Dystrybucja odbywała się zarówno przez e-mail, SMS, jak i reklamy na Facebooku. Przestępcy wyłudzali dane logowania, dane kart płatniczych oraz inne informacje osobowe.

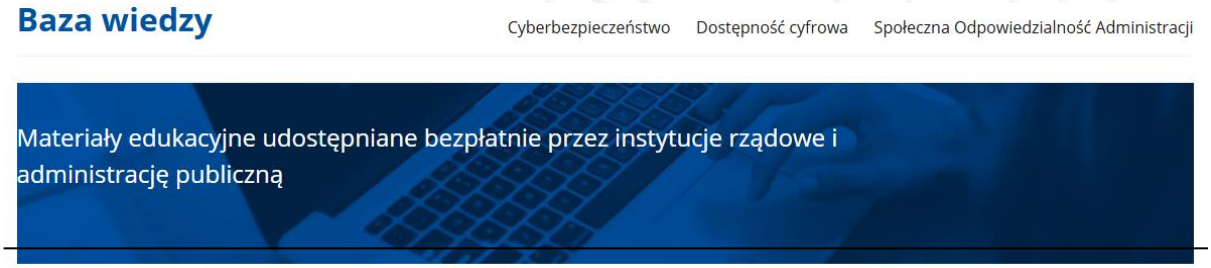
Najskuteczniejszą ochroną nadal pozostaje wiedza i czujność, dlatego zachęcamy do śledzenia naszych profili w mediach społecznościowych oraz portalu https://cebrf.knf.gov.pl.

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:

- Szkolenia - Baza wiedzy - Portal Gov.pl

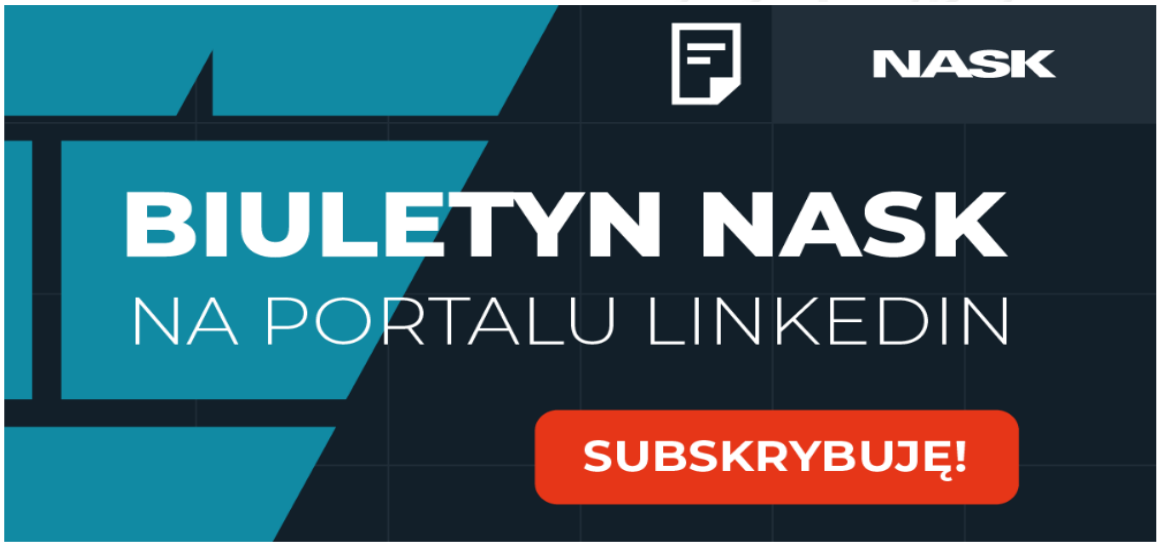


BIULETYN NASK

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

Link do zapisów:

- Aktualności NASK



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.