BRANDEFENSE COUNTRY REPORT · POLAND 2026

Brandefense: raport o krajobrazie cyberzagrożeń w Polsce w 2026 roku

Dane u dostawców, nadużycia tożsamości i odtwarzanie usług w cyfrowej gospodarce

Odin by Brandefense
Okres badania: 1 stycznia–22 listopada 2026, według daty wpisu
Wersja 1.0 · Publiczna edycja badawcza · TLP:CLEAR · 22 listopada 2026

78 z 250
wybranych domen z bieżącą ofertą danych logowania

7
wybranych dossier z odrębnymi granicami twierdzeń

15
szczegółowych kart opartych na źródłach oficjalnych, odrębnych od ofert podziemia

56
polskich wpisów ransomware pod 21 etykietami grup

SPIS TREŚCI

Spis treści

Translated with AI

To wydanie przetłumaczono z pomocą AI z angielskiego tekstu źródłowego. W razie rozbieżności rozstrzygająca jest wersja angielska.

01	Podsumowanie dla kierownictwa	05
	Mapa raportu	09
02	Cyfrowy kontekst i bezpieczeństwo Polski	10
03	Ekspozycja krajowa: wybrany zbiór organizacji	14
04	Co obserwujemy w podziemiu internetowym	23
05	Potwierdzone incydenty i zarzuty według sektorów	39
06	Haktywizm, DDoS i ostatnia aktywność	57
07	Aktorzy zagrożeń i powiązania dowodowe	63
08	Ekonomia oszustw	74
09	Bankowość i finanse	79
10	Regulacje i reakcja instytucji	84
11	Perspektywy	88
12	Plan działania	92
A	Dodatek A. Metoda i granice dowodowe	99
B	Dodatek B. Rejestr dowodów	102
C	Dodatek C. Źródła	103
D	Dodatek D. Słownik	107
	O raporcie	108

Zarząd i CISO	01 05 11 12
SOC i wywiad	04 06 07 12
Tożsamość i infrastruktura	03 05 07 12
Finanse i oszustwa	08 09 12
Prawo i zakupy	05 10 12

O wydaniu

Przetłumaczono z pomocą AI. W razie rozbieżności rozstrzygająca jest wersja angielska.

Badanie i redakcja wspomagane przez AI. Raport odróżnia obserwacje, twierdzenia przestępcze, oficjalne ujawnienia i interpretacje analityczne. Ostatni dzień obserwacji jest częściowy.

Zweryfikowane ujawnienia w Polsce wskazują na dane u dostawców, uprawnienia kont i odtwarzanie usług. Skala i pochodzenie ofert podziemia wymagają sprawdzenia.

118 390

publikacji związanych z krajem [S1]

56

polskich wpisów ransomware [S3]

78 / 250

wybrane domeny z bieżącą ofertą danych logowania [S2]

22

szczegółowych dossier ofert i relacji oficjalnych

Spis treści i ścieżki czytania

Raport przechodzi od decyzji do dowodów, a następnie działań z właścicielami. Dwanaście rozdziałów zachowuje różnice między ogłoszeniem, oficjalnym incydentem i oceną analityczną.

Rozdział	Pytanie	Pierwszy odbiorca
1 Podsumowanie	Co kierownictwo powinno ustalić najpierw?	Zarząd i CISO
2 Kontekst	Które zależności nadają przypadkom znaczenie?	Kierownictwo i architektura
3 Ekspozycja	Co ustalają obserwacje wybranych domen?	Tożsamość i infrastruktura
4 Dowody podziemia	Co deklarują oferty danych i dostępu?	Wywiad i reagowanie
5 Incydenty sektorowe	Które oficjalne relacje zmieniają reakcję?	Właściciele usług i sektorów
6 DDoS i ostatnia aktywność	Co zadeklarowano, potwierdzono i co zmieniło się ostatnio?	Operacje i komunikacja
7 Aktorzy zagrożeń	Które przypisania i związki mają oparcie?	Wywiad i SOC
8 Ekonomia oszustw	Jak prawdziwa informacja wspiera fałszywą dyspozycję?	Ochrona klientów
9 Bankowość	Które decyzje finansowe wymagają współpracy?	Finanse i tożsamość
10 Regulacje	Jakie obowiązki i terminy przejściowe mają zastosowanie?	Prawo i zgodność
11 Perspektywy	Co zmieniłoby ocenę?	Kierownictwo
12 Plan działania	Kto działa i co potwierdza wykonanie?	Wszyscy właściciele

Kierownictwo: rozdziały 1, 5 i 10–12. **Operacje:** rozdziały 4, 6–7 i 12. **Tożsamość i oszustwa:** rozdziały 3, 8–9 i 12.

Zaobserwowano oznacza zachowany wpis lub pomiar. **Zadeklarowano** oznacza twierdzenie autora lub wpisu. **Oficjalnie poinformowano** oznacza ujawnienie organizacji lub organu w podanym zakresie.

Interpretacja analityczna łączy dowód z decyzją. Nie uzupełnia brakującego potwierdzenia dostępu, osób, kierowania państwowego, transakcji ani strat.

ROZDZIAŁ 01

Podsumowanie dla kierownictwa

01

TEN ROZDZIAŁ ODPOWIADA

Które decyzje wynikają bezpośrednio ze zweryfikowanych ujawnień i zachowanych dowodów z Polski?

4

decyzje kierownictwa z odpowiedzialnymi właścicielami

Cztery decyzje kierownictwa 07

Rok w liczbach 07

ROZDZIAŁ 01

Podsumowanie dla kierownictwa

W SKRÓCIE

Dowody z Polski w 2026 łączą informacje u dostawców, nadużycia kont i odtwarzanie usług. Oficjalne komunikaty opisują dane medyczne i księgowe, publikację danych uczelni oraz etapowe przywracanie usług publicznych. Ransompedia zawiera 56 polskich wpisów; oferty podziemia wymagają osobnej weryfikacji. Krajowa ocena Atlas wynosi 51 na 100. Nadaj priorytet zakresowi dostawcy, weryfikacji tożsamości, niezależnej akceptacji płatności i odtwarzaniu kluczowych procesów.

1. Wspólne oprogramowanie rozdziela reakcję między wielu administratorów. Komunikat ministerstwa o MyDr wskazuje możliwy zakres 18,8 miliona osób i ponad 12 000 placówek oraz dane historyczne. FELG i Fakturownia także odróżniają dochodzenie dostawcy od oceny klienta. Populacji nie sumuje się [S5][S8][S10].

2. Działająca usługa nie rozstrzyga incydentu danych. Oficjalna relacja MyDr wskazuje brak przerwy opieki. Uczelnia potwierdza kopiowanie i publikację bez szyfrowania kluczowych systemów. Listopadowa reakcja ePUAP wymagała natomiast przywracania etapami. Dostępność, dostęp, kopiowanie i użycie wymagają osobnych odpowiedzi [S5][S31][S41].

3. Wpisy ransomware uzasadniają odtwarzanie z zachowaniem granic widoczności. Ransompedia zawiera 56 wpisów przypisanych Polsce pod 21 etykietami grup. The Gentlemen odpowiada za 19. Liczba 32 za cały 2025 obejmuje inny okres, a nie zmierzone roczne tempo wzrostu [S3].

4. Ostatnie oferty dostępu wymagają weryfikacji. Listopadowa oferta gastronomiczna deklaruje świeży eksport, a odrębne ogłoszenie skrzynki podmiotu publicznego deklaruje bieżący stan. Żadne nie ustala aktywnego dostępu, liczby osób ani związku z oficjalnymi listopadowymi incydentami. Cena oznacza ofertę, a nie zweryfikowaną sprzedaż [S1].

5. Bieżące oferty danych logowania wymagają weryfikacji kont. Dane logowania powiązane z 78 z 250 wybranych domen były oferowane w momencie sprawdzenia. Krajowa ocena Atlas wynosi 51 na 100. Portfel obejmuje co najmniej 590 940 powiązań urządzeń i 281 292 486 historycznych powiązań rekordów logowania. Nakładające się obserwacje nie ustalają odrębnych osób ani potwierdzonych włamań [S2].

Cztery decyzje kierownictwa

1. **Wymagaj zakresu konkretnego klienta.** Zakupy i IOD powinny uzyskać informacje o koncie lub gabinecie po komunikacie dostawcy. Zachowaj moment stwierdzenia i oceń obowiązki zgłoszenia przed zakończeniem całego dochodzenia.
1. **Weryfikuj uprawnienie konta.** Zespół tożsamości i SOC powinny porównywać właściwe oferty z aktywnymi kontami, sesjami i wcześniejszymi działaniami. Nadaj pierwszeństwo uwierzytelnianiu odpornemu na phishing dla ważnych kont i przetestuj odzyskiwanie.
1. **Chroń wrażliwe dyspozycje.** Finanse i obsługa potrzebują niezależnej weryfikacji zmian odbiorców, pilnych przelewów i rozmów powołujących się na komunikat. Przetestuj proces z prawidłowymi syntetycznymi szczegółami biznesowymi.
1. **Wykaż odtworzenie usługi.** Właściciel biznesowy i infrastruktura powinni wspólnie przeprowadzić ćwiczenie. Uwzględnij chronione kopie, niezależną administrację, integralność, procesy alternatywne i zatwierdzenie rzeczywistego działania usługi.

Rok w liczbach

Wartości opisują różne populacje i nie wolno ich sumować.

118 390

Publikacje związane z krajem w okresie wpisów [S1]

CZEGO NIE OZNACZA

Ataków, celowego wyboru Polski lub odrębnych ofert

119 484

Odrębne zachowane wpisy tego wydania [S1]

CZEGO NIE OZNACZA

Pełnej populacji publikacji

56

Wpisy Ransompedia oznaczone jako Polska [S3]

CZEGO NIE OZNACZA

Potwierdzonego szyfrowania lub niezależnie zweryfikowanych ofiar

78 z 250

Wybrane domeny z ofertą danych logowania w momencie sprawdzenia [S2]

CZEGO NIE OZNACZA

Nie potwierdza dostępu do infrastruktury, poprawności kont lub krajowej częstości

51 / 100

Krajowa ocena Atlas wybranego portfela [S2]

CZEGO NIE OZNACZA

Nie jest oceną sektora lub prawdopodobieństwem ataku

182 z 241

Polityki DMARC żądające kwarantanny lub odrzucenia [S2]

CZEGO NIE OZNACZA

Pełnego egzekwowania lub zapobiegania phishingowi

18,8 miliona

Możliwa populacja MyDr według ministerstwa [S5]

CZEGO NIE OZNACZA

Liczby odrębnych osób niezależnie sprawdzonej przez autorów

455

Karty związane z Polską widoczne jawnie w zachowanych wpisach [S4]

CZEGO NIE OZNACZA

Kradzieży kart, ich ważności, strat ani szerszego zakresu Brandefense

22

Siedem szczegółowych ofert i piętnaście oficjalnych dossier

CZEGO NIE OZNACZA

Pełnej liczby krajowej lub dwudziestu dwóch potwierdzonych włamań

Ostatnia aktywność obejmuje 9–22 listopada. Ostatni dzień i listopad są częściowe. Raport rozróżnia daty ujawnienia, publikacji wpisu i włamania.

NAJWAŻNIEJSZE WNIOSKI

01

Zacznij od zakresu dostawcy, uprawnień kont i odtwarzania usług kluczowych.

02

Zachowuj odrębność wpisów, osób, plików i organizacji.

03

Eskaluj na podstawie potwierdzonych faktów i zachowuj niepewność kopiowania lub wpływu.

Mapa raportu

Wybierz własną decyzję, a następnie przejdź do dowodów i warunku zakończenia.

Zarząd i CISO	Co wymaga finansowania i właściciela?	01 05 11 12
SOC i wywiad	Który zarzut sprawdzić i które źródło uzasadnia przypisanie?	04 06 07 12
Tożsamość i infrastruktura	Które konta, konfiguracje i ścieżki odtwarzania wymagają kontroli?	03 05 07 12
Finanse i oszustwa	Co nigdy nie powinno zatwierdzać zmiany konta lub płatności?	08 09 12
Prawo i zakupy	Kto kontroluje dane i jaki termin obowiązuje?	05 10 12

Ścieżka dowodowa	Pytanie	Granica
Zachowane wpisy	Co jest reklamowane lub ogłaszane?	Twierdzenia wymagają osobnego sprawdzenia
Wpisy ransomware	Co widać w zbiorze źródła?	Wpisy nie są potwierdzonymi incydentami
Obserwacje ekspozycji i pasywne	Które konta, urządzenia i konfiguracje wymagają weryfikacji?	Powiązania i żądania polityk nie dowodzą włamania
Ujawnienia oficjalne	Co podaje organizacja lub organ?	Szacunki i ustalenia mogą się zmieniać
Publiczne badania	Jakie zachowania i przypisania opisuje badacz?	Nadal obowiązują zakres źródła i daty zdarzeń

ROZDZIAŁ 02

Cyfrowy kontekst i bezpieczeństwo Polski

02

TEN ROZDZIAŁ ODPOWIADA

Które zależności sprawiają, że opisane incydenty mają znaczenie dla polskich organizacji?

90,5%

korzystanie z internetu według szacunków z października 2026

2.1 Powszechny dostęp i wiele punktów użycia tożsamości 11

2.2 Wspólne oprogramowanie łączy niezależnych administratorów 11

2.3 Dostępność i poufność wymagają osobnych odpowiedzi 11

2.4 Narracje polityczne i przypisywanie ocen źródłom 12

2.5 Historyczny incydent energetyczny a obecne planowanie 12

2.6 Obowiązki mają konkretny harmonogram 12

ROZDZIAŁ 02

Cyfrowy kontekst i bezpieczeństwo Polski

W SKRÓCIE

Usługi cyfrowe w Polsce gromadzą dane tożsamościowe, medyczne i biznesowe na platformach używanych przez wiele niezależnych organizacji. Tegoroczne komunikaty urzędowe opisują incydenty u dostawców, oszustwa mobilne i długie przywracanie usług publicznych. Oceny powiązań państwowych wymagają innych dowodów niż ogłoszenia przestępcze. Opracuj wykaz usług obejmujący dostawców tożsamości, procesorów i zależności odtwarzania, a następnie przypisz każdej pozycji właściciela.

2.1 Powszechny dostęp i wiele punktów użycia tożsamości

DataReportal opublikował raport Digital 2027 Poland w listopadzie 2026. Październikowe szacunki obejmują 34,2 miliona użytkowników internetu, 90,5% populacji, 54,4 miliona połączeń mobilnych i 28,0 miliona tożsamości w mediach społecznościowych. Połączenia i tożsamości nie oznaczają odrębnych osób [S29].

Te liczby wyjaśniają znaczenie zależności między usługami, a nie prawdopodobieństwo ataku. Pacjent, pracownik lub przedsiębiorca może podawać te same dane kontaktowe w systemach medycznych, księgowych, bankowych i publicznych. Ujawniony adres może więc uwiarygodnić późniejszą wiadomość oszusta.

Dane identyfikacyjne powinny pomagać znaleźć właściwy rekord. Nie powinny uprawniać do resetowania hasła, zmiany rachunku bankowego ani ujawnienia informacji medycznych. Ta zasada pozostaje przydatna także wtedy, gdy dane pochodzą sprzed kilku lat.

2.2 Wspólne oprogramowanie łączy niezależnych administratorów

Komunikaty MyDr i FELG dotyczą oprogramowania używanego przez niezależne gabinety. Fakturownia odróżnia dane, których jest administratorem, od informacji powierzonych przez klientów do przetwarzania. Incydent u dostawcy może zatem wymagać wielu odrębnych ocen i decyzji o zgłoszeniu naruszenia [S5][S8][S10].

Sam wykaz zakupionych usług nie pokazuje tej zależności. Przydatny rejestr wskazuje aplikację, kategorie danych, administratora, procesora, podwykonawców, konta administracyjne i proces biznesowy. Określa też osobę odpowiedzialną za uzyskanie oceny dotyczącej konkretnego konta po ogólnym komunikacie dostawcy.

Nie oznacza to, że dane każdego klienta dostawcy zostały ujawnione. Platforma, konto klienta, gabinet, rekord i osoba to różne jednostki. Raport zachowuje te rozróżnienia.

2.3 Dostępność i poufność wymagają osobnych odpowiedzi

Komunikat ministerstwa dotyczący MyDr stwierdzał brak zakłóceń bieżącej opieki, w tym wystawiania recept. Po listopadowym incydencie usługi ePUAP przywracano etapami. Te relacje pokazują różne skutki dla działania usług [S5][S31].

Usługa może działać mimo nieuprawnionego dostępu do danych historycznych. Ograniczenia zapobiegawcze mogą też utrzymywać się po zatrzymaniu bezpośredniego zagrożenia. Żadna z tych sytuacji sama nie przesądza, czy skopiowano dane osobowe.

Właściciele procesów powinni przygotować dwie oceny: jakie zadania można wykonywać i jakie informacje mogły zostać ujawnione. Komunikaty powinny przedstawiać każdą odpowiedź wraz z jej podstawą i czasem aktualizacji.

2.4 Narracje polityczne i przypisywanie ocen źródłom

CERT Polska wskazuje UNC1151/Ghostwriter w czerwcowym raporcie o phishingu. W styczniowym raporcie energetycznym porównuje infrastrukturę z nazwanym klastrem aktywności. ZeroFox opisuje deklaracje DDoS dotyczące Polski, którym towarzyszy narracja polityczna. To oceny tych źródeł w określonym zakresie [S14][S18] [S30].

Rosyjskojęzyczne ogłoszenie nie dowodzi rosyjskiego pochodzenia operatora, kierowania przez państwo ani związku ze służbą wywiadowczą. Dotyczy to również odniesień białoruskich, tematów ukraińskich, haseł patriotycznych i twierdzeń o wyborach. Język, deklarowany motyw, powiązanie techniczne i przypisanie państwu odpowiadają na inne pytania.

Raport nie zajmuje stanowiska wobec decyzji władz, stosunków międzynarodowych ani sporów politycznych. Nie wywodzi przyczyny incydentu z polityki krajowej. Przypisanie sprawstwa jest przedstawiane jako ocena konkretnego źródła, a nie niezależnie ustalony wniosek.

2.5 Historyczny incydent energetyczny a obecne planowanie

Styczniowy raport CERT Polska dotyczy ataków z 29 grudnia 2025. Opisuje co najmniej 30 obiektów OZE, przedsiębiorstwo produkcyjne i elektrociepłownię. Według raportu produkcja energii i dostawy ciepła nie zostały przerwane zgodnie z zamiarem sprawcy [S18].

Zdarzenia poprzedzają okres objęty raportem. Styczniowa publikacja i późniejsze uzupełnienie są istotnymi ujawnieniami z 2026, lecz nie zmieniają ich w nowe ataki z 2026. Nie powiększają liczby tegorocznych przypadków.

Operatorzy powinni sprawdzić, czy odtwarzanie obejmuje urządzenia terenowe, zdalne zarządzanie i łączność, a nie tylko serwery. Przywrócenie sieci biurowej nie dowodzi możliwości bezpiecznego sterowania procesem przemysłowym.

2.6 Obowiązki mają konkretny harmonogram

Nowelizacja KSC weszła w życie 3 kwietnia 2026. Ministerstwo opublikowało następnie terminy rejestracji, wdrożenia i audytów. Szczegółowe wyjaśnienia odróżniają nowe podmioty kluczowe od dotychczasowych operatorów z trwającym cyklem audytowym [S25][S26].

Na dzień odcięcia termin 3 października już upłynął dla podmiotów spełniających wskazane warunki. Termin wdrożenia przypadający 3 kwietnia 2027 był jeszcze przed nimi. Zespoły prawne powinny ustalić status organizacji i właściwe przepisy przejściowe, zamiast uznawać wszystkie daty za powszechne odroczenia.

NAJWAŻNIEJSZE WNIOSKI

01

Mapuj procesorów i odzyskiwanie tożsamości razem z aplikacjami i serwerami.

02

Oddziel działającą usługę od ustaleń dotyczących poufności danych.

03

Zachowaj rozróżnienie między zdarzeniami historycznymi, ocenami powiązań państwowych a tegorocznymi incydentami.

ROZDZIAŁ 03

Ekspozycja krajowa: wybrany zbiór organizacji

TEN ROZDZIAŁ ODPOWIADA

Jaka ekspozycja dotyczy wybranych domen i od czego zacząć weryfikację?

78 z 250

wybranych domen z bieżącą ofertą danych logowania

3.1 Karta populacji 15
3.2 Krajowa ocena Atlas i obserwacje sektorowe 16
3.3 Urządzenia i historyczne rekordy logowania 17
3.4 Bieżące oferty wymagają weryfikacji kont 19
3.5 Dokumenty, domeny podobne i wzmianki 19
3.6 Obserwacje uwierzytelniania poczty 20
3.7 Obserwacje DNS, TLS i stron 21
3.8 Weryfikacja przed ustalaniem priorytetów 22

ROZDZIAŁ 03

Ekspozycja krajowa: wybrany zbiór organizacji

W SKRÓCIE

Dane logowania powiązane z 78 z 250 wybranych domen były oferowane w momencie sprawdzenia. Krajowa ocena Atlas wynosi 51 na 100. Portfel obejmuje co najmniej 590 940 powiązań urządzeń i 281 292 486 historycznych powiązań rekordów logowania. Obserwacje nakładają się i nie ustalają odrębnych osób ani potwierdzonych włamań. Najpierw sprawdź bieżące konta i sesje, następnie urządzenia pracowników oraz uwierzytelnianie poczty.

3.1 Karta populacji

Lista opisuje kandydackie powiązania z organizacjami. Właściciel prawny, niezależność podmiotów i kompletność aliasów wymagają dalszej weryfikacji. Wyniki dotyczą portfela, a nie krajowej częstości zdarzeń lub zweryfikowanego rankingu organizacji [S2].

Element	Definicja
Wybrany zbiór	250 domen kandydackich z dwunastu sektorów publicznych i prywatnych; jedna główna domena dla kandydata
Wybór	Celowy, według roli instytucjonalnej i znaczenia sektora; nie jest oficjalnym rankingiem przychodów
Populacja pasywna	241 domen z obserwacjami pasywnymi; 9 kandydatów bez takich obserwacji
Populacja ekspozycji	250 domen z obserwacjami ekspozycji; powiązanie źródłowe nie ustala bieżącego właściciela prawnego
Daty	Dane ekspozycji odczytano 21 listopada 2026; dodatkowe liczby źródłowe i obserwacje pasywne odczytano 22 listopada 2026
Okresy	Urządzenia, dane logowania, dokumenty i oferty opisują zasób w momencie sprawdzenia, także historyczny. Wzmianki obejmują poprzednie 365 dni do 22 listopada; domeny podobne obejmują 30 dni do 21 listopada
Nakładanie	Powiązania nie oznaczają odrębnych osób lub urządzeń między źródłami i organizacjami; to samo konto lub urządzenie może dotyczyć wielu domen
Granica wnioskowania	Brak estymacji krajowej częstości, liczby potwierdzonych włamań i skuteczności zabezpieczeń

3.2 Krajowa ocena Atlas i obserwacje sektorowe

Dane logowania związane z 78 z 250 wybranych domen były oferowane w momencie sprawdzenia [S2].

Krajowa ocena Atlas dla wybranego portfela wynosi 51 w skali od 0 do 100. Wyższe wartości oznaczają większą zaobserwowaną ekspozycję. Raport publikuje wyłącznie tę ocenę krajową. Tabela sektorowa pokazuje liczby sygnałów, bez ocen sektorów lub organizacji [S2].

51 / 100

krajowa ocena Atlas wybranego portfela

78 / 250

wybrane domeny z bieżącą ofertą danych logowania

246 / 250

wybrane domeny z historycznymi rekordami logowania

Mapa porównuje występowanie osobnych sygnałów. Bieżąca oferta oznacza dane logowania związane z domeną oferowane w momencie sprawdzenia; historia dotyczy wcześniejszych ofert. Żadna nie ustala poprawności konta ani zakończonej sprzedaży.

Bieżące oferty i powiązania urządzeń pracowników różnią się między sektorami

Wybrane domeny z danym sygnałem względem mianownika sektora. Bieżące oferty danych logowania pokazano kolorem koralowym.

	Urządzenia	Urządzenia pracowników	Rekordy logowania	Bieżące oferty	Historia ofert	Podobne domeny	Dokumenty
Bankowość i finanse	29/30	21/30	30/30	10/30	10/30	28/30	15/30
Edukacja	30/30	29/30	30/30	14/30	13/30	29/30	24/30
Energia i usługi komunalne	20/20	17/20	19/20	5/20	4/20	16/20	8/20
Administracja	49/50	38/50	49/50	7/50	7/50	47/50	36/50
Ochrona zdrowia	10/10	7/10	10/10	4/10	4/10	10/10	4/10
Hotelarstwo i turystyka	8/10	6/10	10/10	4/10	4/10	9/10	5/10
Ubezpieczenia	10/10	8/10	10/10	4/10	4/10	9/10	6/10
Produkcja i przemysł	25/30	22/30	29/30	2/30	2/30	17/30	10/30
Media i rozrywka	10/10	7/10	10/10	4/10	4/10	10/10	9/10
Handel i holdingi	18/20	18/20	19/20	15/20	15/20	18/20	15/20
Telekomunikacja i technologia	10/10	9/10	10/10	4/10	4/10	10/10	6/10
Transport i logistyka	20/20	14/20	20/20	5/20	5/20	15/20	8/20

Źródło: obserwacje ekspozycji Brandefense dla 250 wybranych domen kandydackich, odczyt 21 listopada 2026. Kumulatywne powiązania mogą się nakładać; nie ustalają odrębnych osób ani potwierdzonych włamań [S2].

Wszystkie kolumny sygnałów podają liczbę domen kandydackich. W plikach H01 i C04 `candidate_domains` oznacza liczbę wybranych domen w sektorze. Kolumna `candidate_domains_with_listing_history` w H01 liczy domeny z wcześniejszymi ofertami, a nie pojedyncze oferty.

Sektor	Domeny	Domeny z bieżącymi ofertami	Domeny z historią ofert	Domeny z powiązaniami urządzeń pracowników	Domeny z odniesieniami do dokumentów
Administracja	50	7	7	38	36
Bankowość i finanse	30	10	10	21	15
Edukacja	30	14	13	29	24
Produkcja i przemysł	30	2	2	22	10
Energia i usługi komunalne	20	5	4	17	8
Handel i holdingi	20	15	15	18	15
Transport i logistyka	20	5	5	14	8
Telekomunikacja i technologia	10	4	4	9	6
Ochrona zdrowia	10	4	4	7	4
Ubezpieczenia	10	4	4	8	6
Hotelarstwo i turystyka	10	4	4	6	5
Media i rozrywka	10	4	4	7	9
Wszystkie wybrane	250	78	76	196	146

3.3 Urządzenia i historyczne rekordy logowania

C04 oddziela powiązania urządzeń klasyfikowanych jako pracownicze od pozostałych. Właściciela pozostałych urządzeń nie ustalono; możliwe są konta klientów, studentów, wykonawców i konta historyczne [S2].

Powiązania urządzeń obejmują usługi konsumenckie, instytucje publiczne i edukację



Źródło: obserwacje ekspozycji Brandefense dla 250 wybranych domen kandydackich, odczyt 21 listopada 2026. Kumulatywne powiązania mogą się nakładać; nie ustalają odrębnych osób ani potwierdzonych włamań [S2].

Sektor	Domeny z urządzeniami	Powiązania urządzeń	Powiązania pracowników	Rekordy logowania
Handel i holdingi	18 / 20	150 175	669	57 439
Administracja	49 / 50	81 900	2 143	273 278
Bankowość i finanse	29 / 30	80 757	304	54 584
Media i rozrywka	10 / 10	71 762	40 154	271 636 420
Telekomunikacja i technologia	10 / 10	64 754	646	8 537 438
Energia i usługi komunalne	20 / 20	36 293	140	26 862
Edukacja	30 / 30	30 003	3 652	596 069
Ubezpieczenia	10 / 10	23 680	93	28 064
Transport i logistyka	20 / 20	23 550	251	29 373
Ochrona zdrowia	10 / 10	13 151	32	10 971
Produkcja i przemysł	25 / 30	10 484	174	30 899
Hotelarstwo i turystyka	8 / 10	4 431	42	11 089
Wszystkie wybrane	239 / 250	590 940	48 300	281 292 486

Część sum urządzeń jest dolnymi granicami. Powiązania pracowników mieszczą się w sumie urządzeń i nie należy ich dodawać. Historyczne rekordy mogą powtarzać konta, osoby i starsze dane; nie wskazują aktywnych danych logowania.

Populacja obejmuje 89 719 574 rekordów baz naruszeń, 15 418 280 rekordów stealera i 176 154 632 wpisów combolist. Powiązania źródłowe nie są liczbą polskich mieszkańców. Dużą sumę mediów i rozrywki należy sprawdzić w jej zakresie źródłowym i kontowym.

≥590 940

powiązania urządzeń, w tym klasyfikowanych jako pracownicze

48 300

powiązania urządzeń klasyfikowanych jako pracownicze

281 292 486

historyczne powiązania rekordów logowania

3.4 Bieżące oferty wymagają weryfikacji kont

Dane logowania powiązane z 78 z 250 wybranych domen były oferowane w momencie obserwacji. Konto może należeć do klienta, pracownika lub innego użytkownika. Oferta nie ustala dostępu do infrastruktury organizacji [S2].

Zespół tożsamości powinien sprawdzić aktywność konta, wcześniejsze działania naprawcze oraz podejrzane sesje lub zmiany odzyskiwania. Przed odebraniem dostępu lub wymuszeniem zakłócającej zmiany hasła sprawdź właściciela i aktualność.

3.5 Dokumenty, domeny podobne i wzmianki

Tabela opisuje odniesienia i kandydatów podobieństwa, a nie potwierdzone ujawnienie wrażliwych dokumentów lub złośliwe domeny. Dokument może być publiczny, przestarzały lub niezwiązany z aktywnym systemem. Podobną nazwę musi zweryfikować właściciel [S2].

Sektor	Dokumenty	Domeny podobne	Domeny z podobieństwami
Administracja	8 253	10 818	47
Bankowość i finanse	56	4 883	28
Edukacja	133	25 129	29
Produkcja i przemysł	25	1 066	17
Energia i usługi komunalne	10	6 036	16

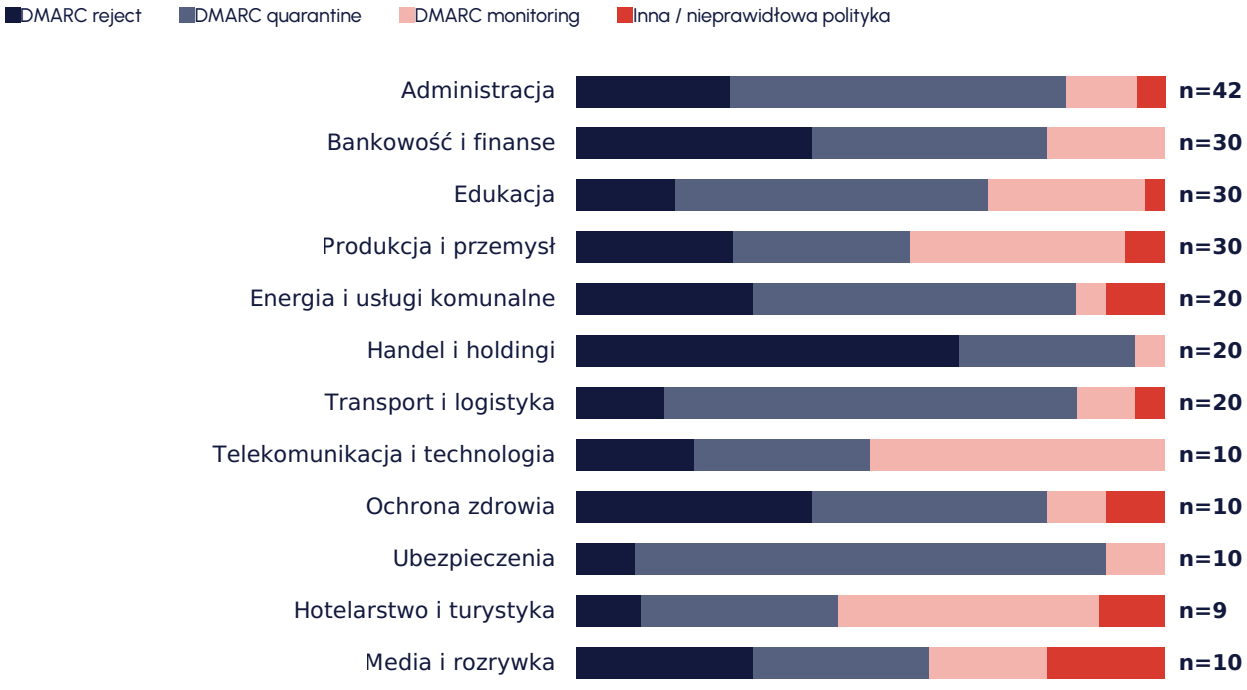
Sektor	Dokumenty	Domeny podobne	Domeny z podobieństwami
Handel i holdingi	91	7 506	18
Transport i logistyka	61	16 608	15
Telekomunikacja i technologia	66	21 542	10
Ochrona zdrowia	4	798	10
Ubezpieczenia	12	555	9
Hotelarstwo i turystyka	66	2 641	9
Media i rozrywka	1 333	996	10
Wszystkie wybrane	10 110	98 578	218

Wybrane domeny mają 2 518 wzmianek w źródłach rozmów i 998 w źródłach sieciowych w poprzednich 365 dniach. Wzmianki mogą obejmować komentarze, reklamy i powtórzenia. Nie mierzą odrębnych sprawców, ataków lub potwierdzonego dostępu.

3.6 Obserwacje uwierzytelniania poczty

Obserwacje pasywne mają własny mianownik. Wykres pokazuje żądaną politykę poczty, bez pomiaru przyjmowania, skuteczności podszywania się lub wdrożenia u każdego prawidłowego nadawcy.

Żądania polityk DMARC różnią się między wybranymi sektorami



Źródło: publiczne obserwacje pasywne 241 wybranych domen, odczyt 22 listopada 2026. Każdy sektor ma własny mianownik obserwowanych domen; żądania polityk nie potwierdzają egzekwowania [S2].

Sektor	Domeny	Kwarantanna lub odrzucenie	Monitorowanie	Inne lub niezaobserwowane
Administracja	42	35	5	2
Bankowość i finanse	30	24	6	0
Edukacja	30	21	8	1
Produkcja i przemysł	30	17	11	2
Energia i usługi komunalne	20	17	1	2
Handel i holdingi	20	19	1	0
Transport i logistyka	20	17	2	1
Telekomunikacja i technologia	10	5	5	0
Ochrona zdrowia	10	8	1	1
Ubezpieczenia	10	9	1	0
Hotelarstwo i turystyka	9	4	4	1
Media i rozrywka	10	6	2	2
Wszystkie obserwowane	241	182	47	12

Liczba 182 żądań kwarantanny lub odrzucenia odpowiada 75,5% z 241 obserwowanych domen. Obejmuje 69 polityk odrzucenia i 113 kwarantanny. Nie ustala pełnego wdrożenia, zgodności lub egzekwowania przez odbiorców [S2].

Rekordy SPF zaobserwowano dla 237 domen, a rekordy podpisywania DKIM dla 154. Brak obserwacji nie dowodzi, że domena nigdy nie podpisuje poczty. Przed zmianą dostarczania porównaj rzeczywistych nadawców i wyniki uwierzytelniania.

3.7 Obserwacje DNS, TLS i stron

Wyniki nierozstrzygające nie są udaną walidacją ani potwierdzoną awarią zabezpieczenia. Każdy wiersz zachowuje własny mianownik [S2].

Obserwacja	Wynik	Granica interpretacji
Rekord delegacji DNSSEC	20 z 241	Sama delegacja nie ustala poprawnej walidacji całego łańcucha
Rozstrzygająca walidacja TLS	234 z 241	7 wyników było nierozstrzygających
Udana walidacja TLS	227 z 234	Obserwowane połączenie, nie każda usługa lub klient
Błędy walidacji TLS	7 z 234	Wymagają sprawdzenia przez właściciela; nie dowodzą nieuprawnionego dostępu
Odpowiedzi strony głównej	196 z 241	Odpowiedź nie jest oceną własności lub bezpieczeństwa aplikacji
Zaobserwowany HSTS	129 z 196	Tylko odpowiadające strony; nie każda subdomena lub użytkownik

3.8 Weryfikacja przed ustalaniem priorytetów

Zespół tożsamości powinien dopasować sygnał zewnętrzny do aktywnego konta i sesji. Badanie urządzeń pracowników i ochrona kont klientów wymagają osobnych właścicieli. Same historyczne rekordy nie uzasadniają stwierdzenia bieżącego włamania.

Właściciele poczty powinni ustalić prawidłowych nadawców i zgodność uwierzytelniania przed zaostrzeniem polityki. Zakończenie wymaga prawidłowego dostarczenia legalnej poczty i odrzucenia nieuprawnionego użycia w uzgodnionym teście. Sam rekord nie wykazuje tego wyniku.

Właściciele infrastruktury powinni porównać błędy i wyniki nierozstrzygające z własną konfiguracją. Przekierowania, stare domeny i granice organizacyjne mogą zmienić właściwy wykaz. Nie wyprowadzono związku przyczynowego między konfiguracją a incydentem.

NAJWAŻNIEJSZE WNIOSKI

01

Porównuj bieżące oferty z aktywnymi kontami i dowodami sesji.

02

Zachowaj odrębny zakres urządzeń pracowników, innych urządzeń i historycznych rekordów logowania.

03

Korzystaj z krajowej oceny Atlas razem z sygnałami i zweryfikowaną własnością.

ROZDZIAŁ 04

Co obserwujemy w podziemiu internetowym

04

TEN ROZDZIAŁ ODPOWIADA

Co ustalają polskie oferty danych i dostępu, a co nadal wymaga sprawdzenia?

7

wybranych dossier z odrębnymi granicami twierdzeń

4.1 Karta popularności 24
4.2 Wielkość, platformy i język 24
4.3 Przykładowe obserwacje rodzajów aktywności 26
4.4 Oferty związane z Polską 27
4.5 Przypadek A: oferta dostępu do usługi publicznej (B01) 28
4.6 Przypadek B: rzekomy wyciąg kont pacjentów (B02) 29
4.7 Przypadek C: ostatnia oferta danych gastronomicznych (B03) 30
4.8 Przypadek D: oferta podróżna z niejasnym mianownikiem kraju (B04) 31
4.9 Przypadek E: użytkownicy i wiersze bazy to różne wielkości (B05) 32
4.10 Przypadek F: powtarzana promocja danych sklepu (B06) 33
4.11 Czego zachowane dowody nie łączą 34
4.12 Dodatkowe oferty i usługi z motywem administracji 34
4.13 Przypadek U: pliki telekomu i dostęp do pomocy (B12) 36
4.14 Mniejsze bazy i reklamy uprzywilejowanego dostępu 37

ROZDZIAŁ 04

Co obserwujemy w podziemiu internetowym

W SKRÓCIE

Wpisy związane z Polską reklamują dostęp, rekordy klientów, materiały tożsamościowe i konta. Siedem dossier pokazuje potrzebę rozdzielania wielkości, aktualności i pochodzenia. Rekordy podróżne nie muszą dotyczyć polskich mieszkańców, wiersze zamówień nie są osobami, a dane logowania pacjentów nie dowodzą włamania do dostawcy. Sprawdź istotną ofertę we własnych danych kont i systemów przed przyjęciem deklarowanej skali.

4.1 Karta populacji

Liczby publikacji i zachowana treść opisują różne populacje. Sam związek z krajem nie dowodzi celowego atakowania Polski [S1].

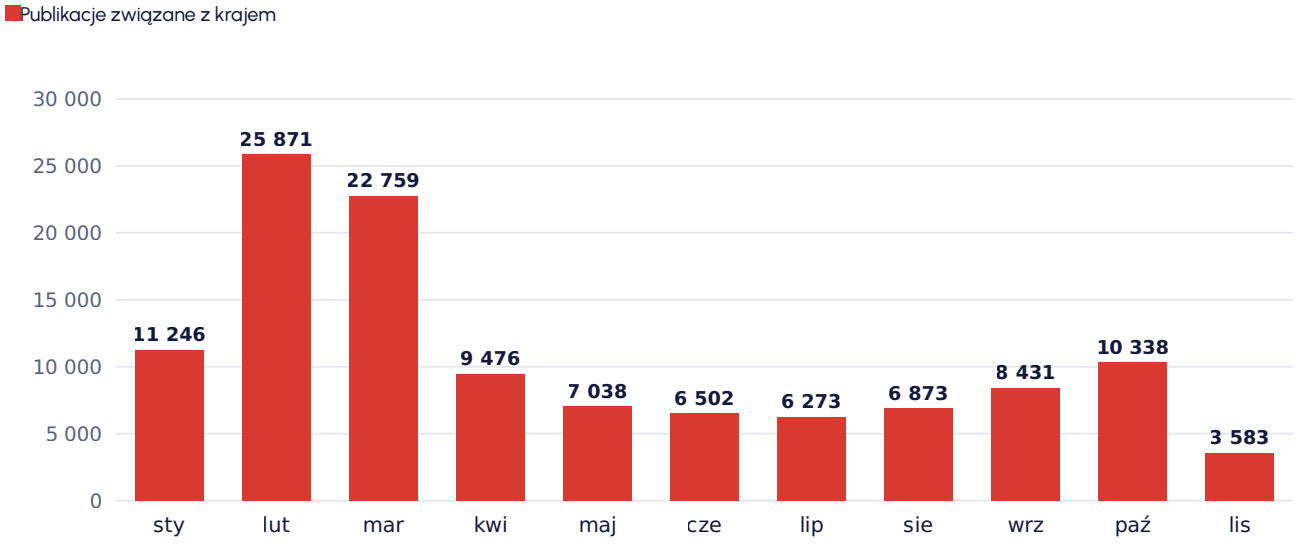
Element	Populacja lub granica
Okres	1 stycznia–22 listopada 2026, według daty wpisu; ostatni dzień jest częściowy
Publikacje związane z krajem	118 390 oznaczonych wpisów; obejmują ogłoszenia, komentarze i powtórzenia
Zachowana treść	119 484 odrębnych wpisów ze zbioru krajowego i materiałów powiązanych
Zachowane platformy	1 434 forum, 117 911 Telegram, 69 paste, 70 Discord
Ostatnia zachowana populacja	2 123 wpisów z 9–22 listopada; nie jest krajową liczbą incydentów
Wybrane przypadki	Siedem ofert A–F i U wspartych kartami B01–B06 i B12
Nie ustalono	Autentyczności pliku, aktywnego dostępu, odrębnych osób, zakończonej sprzedaży ani częstości incydentów w kraju

Zachowana treść związana z krajem zawiera 118 387 wpisów w populacji 118 390 publikacji. Zakres powiązanych źródeł pozostaje częściowy. Raport nie przelicza kategorii zachowanych wpisów na krajowe liczby przestępstw.

4.2 Wielkość, platformy i język

Wykres miesięczny pokazuje populację publikacji, a nie nowe incydenty. Luty obejmuje 25 871 wpisów, a marzec 22 759. Listopad ma 3 583 w chwili obserwacji i jest niepełny [S1].

Publikacje związane z krajem nie tworzą krajowego trendu incydentów



Źródło: zachowane publikacje Brandefense związane z Polską, 1 stycznia–22 listopada 2026; listopad niepełny. Etykiety języka mogą się nakładać; publikacje nie są liczbą incydentów [S1].

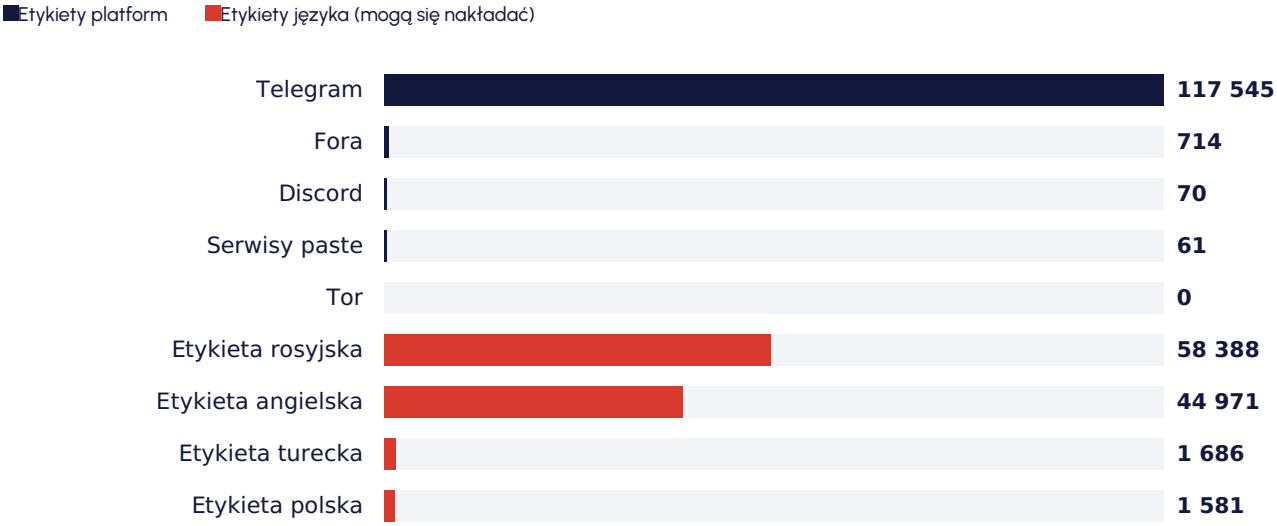
Zmiany mogą wynikać z reklam, widoczności źródeł i zakresu gromadzenia. Wykres nie dowodzi szczytu ataków w lutym ani poprawy bezpieczeństwa po spadku. Wpisy mogą dotyczyć starszych danych lub wymieniać wiele krajów jednocześnie.

W zachowanym materiale przeważają Telegram i fora. Opisuje to zachowany zbiór, a nie znaczenie wszystkich miejsc handlu. Zamknięte wymiany, usunięte treści i prywatne transakcje pozostają poza dowodami.

W zachowanym materiale występują angielski, rosyjski, polski i turecki. Etykiety języka mogą się nakładać i zawierać niespójności. Wydanie nie szacuje więc narodowości przestępców na podstawie języka ani nie tworzy rankingu krajowych rynków językowych.

Populacja publikacji ma poniższe obserwacje platform i języków. Etykiety języka mogą się nakładać; liczb nie należy sumować. To etykiety publikacji, a nie narodowość przestępców lub liczba sprawców [S1].

Etykiety platform i języków opisują publikacje, a nie zweryfikowanych sprawców



Źródło: zachowane publikacje Brandefense związane z Polską, 1 stycznia–22 listopada 2026; listopad niepełny. Etykiety języka mogą się nakładać; publikacje nie są liczbą incydentów [S1].

Wymiar	Etykieta	Publikacje
Platforma	Telegram	117 545
Platforma	Fora	714
Platforma	Discord	70
Platforma	Serwisy paste	61
Platforma	Tor	0
Etykieta języka	Etykieta angielska	44 971
Etykieta języka	Etykieta polska	1 581
Etykieta języka	Etykieta rosyjska	58 388
Etykieta języka	Etykieta turecka	1 686

4.3 Przykładowe obserwacje rodzajów aktywności

Opisowa ocena treści wskazuje 43 320 potencjalnie istotnych wpisów wśród 118 387 zachowanych wpisów związanych z krajem. Kategorie nakładają się. Tabela opisuje tę populację treści, bez estymacji krajowej częstości przestępstw [S1].

Rodzaj aktywności	Wpisy	Co sugeruje	Czego nie ustala
Handel kontami finansowymi	15 496	Reklamowanie kont i dostępu płatniczego	Zakończonych transakcji lub wartości wypłat

Rodzaj aktywności	Wpisy	Co sugeruje	Czego nie ustala
Oferty danych i baz	12 028	Wartość reklamową rekordów tożsamości i biznesu	Nowych poszkodowanych lub pierwotnego źródła
Dokumenty i materiały weryfikacyjne	9 458	Zainteresowanie kontrolą tożsamości	Autentycznych dokumentów lub skutecznej weryfikacji
Phishing i oszustwa	5 944	Promowanie usług i narzędzi	Ich użycia przeciw polskiej organizacji
Materiały związane z kartami	6 179	Obecność tematu kart	Odrębnych kart lub strat
Oferty początkowego dostępu	823	Reklamowanie dostępu jako produktu	Bieżącej kontroli wskazanej organizacji
Zestawy danych logowania	1 245	Dystrybucję kolekcji danych dostępowych	Poprawności kont lub metody pozyskania

Nie wolno sumować wierszy. Jeden wpis może reklamować kilka produktów. Wpisy o kartach są także inną populacją niż odrębne karty z rozdziału 8.

4.4 Oferty związane z Polską

Wybrane dossier zachowują jednostki reklamodawców. Żadne z siedmiu twierdzeń nie jest traktowane jako oficjalnie potwierdzony incydent.

Karta	Publikacja	Ogólna rola celu	Reklamowana jednostka	Status
B01	2026-02-27	Organizacja usług publicznych	Dostęp; ponad dziesięć domen; 200 USD	Dostęp i własność niezweryfikowane
B02	2026-08-21	Usługa medyczna	116 rekordów danych logowania	Poprawność, dostęp i ekspozycja danych zdrowotnych niezweryfikowane
B03	2026-11-15	Usługa gastronomiczna	Deklarowany zbiór 72K	Jednostka wielkości i aktualność niezweryfikowane
B04	2026-05-11	Pośrednik podróżny	Deklarowane 10,3 miliona rekordów	Liczba polskich mieszkańców i pochodzenie niezweryfikowane
B05	2026-01-05	Platforma zamówień	Deklarowane 239 434 użytkowników i 7 456 341 wierszy	Odrębne jednostki, obie niezweryfikowane

Karta	Publikacja	Ogólna rola celu	Reklamowana jednostka	Status
B06	2026-02-02	Sprzedawca internetowy	Deklarowane 100K wierszy	Odrębni klienci i data pozyskania niezweryfikowane
B12	2026-03-20	Usługa telekomunikacyjna	Około 29 578 plików; 17 556 wierszy użytkowników; 51 936 wierszy zgłoszeń	Jednostki, autentyczność i bieżący dostęp do pomocy niezweryfikowane

4.5 Przypadek A: oferta dostępu do usługi publicznej (B01)

Karta dowodowa B01 27 lut 2026

metadata Forum Forum Angielski

ORYGINAŁ

10+ domains hosted on this server Database, secret document, etc $200 in XMR or BTC

TŁUMACZENIE

Ponad 10 domen na tym serwerze. Baza, dokumenty [...] 200 USD w XMR lub BTC.

Zachowany materiał
Zachowano ofertę dostępu do serwera, dokumentów i baz z deklaracją ponad dziesięciu domen.

Nie ustalono
Nie ustalono bieżącego dostępu, własności, wrażliwości dokumentów ani kopiowania.

A

PRZYPADEK A

Oferta dostępu do usługi publicznej

Karta dowodowa B01 | 27 lut 2026 | Forum | Administracja

Niezweryfikowane ogłoszenie

DEKLARACJA	Ogłoszenie z 27 lutego oferowało dostęp do serwera związanego z organizacją usług publicznych. Podawało ponad dziesięć hostowanych domen, bazy i dokumenty oraz cenę 200 USD.
ZACHOWANY MATERIAŁ	Wpis zawiera opis dostępu i wyjście systemu operacyjnego. Materiał potwierdza istnienie i treść reklamy. Nie jest niezależnie odtworzonym testem dostępu.
CO POZOSTAJE NIEZWERYFIKOWANE	Bieżący dostęp, własność, charakter dokumentów i kopiowanie pozostają nieustalone. Liczba domen nie oznacza liczby objętych organizacji. Na potrzeby raportu nie otwierano odnośnika dokumentu ani nie testowano oferowanego konta.

ALTERNATYWY	Wspólny hosting, powtórzony dostęp, niepowiązany klient lub spreparowane wyjście pasowałyby do ogłoszenia. Związek z administracją wymaga sprawdzenia konkretnego zasobu i konta.
REAKCJA	Właściciele usług publicznych powinni zinwentaryzować hosting i administrację, także wykonawców. Przed zakłócającym działaniem dopasuj sygnał do własnego zasobu i aktywnego konta. Zachowaj uzasadnienie końcowej decyzji.

Wniosek

Nie ustalono bieżącego dostępu, własności, wrażliwości dokumentów ani kopiowania.

4.6 Przypadek B: rzekomy wyciąg kont pacjentów (B02)

Karta dowodowa B02 21 sie 2026

updap Forum Forum Angielski

ORYGINAŁ

patient accounts. Users have access to personal medical records, appointment history, lab results, and more. No MFA
Records: 116

TŁUMACZENIE

Konta pacjentów. Dostęp do dokumentacji, historii wizyt, wyników [...] Brak MFA. Rekordy: 116.

Zachowany materiał

Ogłoszenie deklaruje 116 rekordów danych logowania pacjentów i brak MFA.

Nie ustalono

Nie ustalono poprawności danych, liczby osób, dostępu medycznego ani zabezpieczeń dostawcy.

B

PRZYPADEK B

Rzekomy wyciąg kont pacjentów

Karta dowodowa B02 | 21 sie 2026 | Forum | Ochrona zdrowia

Niezweryfikowane ogłoszenie

DEKLARACJA	Wpis z 21 sierpnia reklamował 116 rekordów danych logowania pacjentów. Deklarował dostęp do informacji medycznych i brak MFA. To twierdzenia autora, także w zakresie zabezpieczeń.
ZACHOWANY MATERIAŁ	Wpis opisuje format kolekcji danych logowania i dostęp wymagający punktów forum. Format nie ustala źródła danych. Nie pozyskiwano ani nie testowano reklamowanych rekordów.

ALTERNATYWY	Ponownie użyte hasła, dane z urządzeń, nieaktywne konta lub fikcyjne wpisy pasują do opisu bez włamania do systemu dostawcy. Ani liczby rekordów, ani zakresu medycznego nie ustalono niezależnie.
REAKCJA	Zespół tożsamości dostawcy powinien sprawdzić właściwe konta i sesje w uprawnionym procesie. Prywatność powinna badać dostęp medyczny tam, gdzie uzasadniają to dowody. Raport nie wywodzi braku MFA u dostawcy z ogłoszenia.

Wniosek

Nie ustalono poprawności danych, liczby osób, dostępu medycznego ani zabezpieczeń dostawcy.

4.7 Przypadek C: ostatnia oferta danych gastronomicznych (B03)

Karta dowodowa B03 — 15 lis 2026

Sophia | Forum | Forum | Angielski

ORYGINAŁ

Restaurant with Online Ordering and Delivery in Poland [...] Date of the last database export:2026-11-15

TŁUMACZENIE

Restauracja z zamówieniami i dostawą w Polsce [...] Ostatni eksport bazy: 2026-11-15.

Zachowany materiał

Ogłoszenie deklaruje zbiór 72K i eksport 15 listopada. Nagłówki dotyczą zamówień i kontaktów.

Nie ustalono

Nie ustalono autentyczności, aktualności, liczby osób ani danych kart.

PRZYPADEK C

C

Ostatnia oferta danych gastronomicznych

Karta dowodowa B03 | 15 lis 2026 | Forum | Usługi konsumenckie

Niezweryfikowane ogłoszenie

DEKLARACJA	Ogłoszenie z 15 listopada oferowało zbiór gastronomiczny oznaczony 72K i deklarowało eksport tego samego dnia. Nagłówki tabel dotyczyły kontaktów, adresów dostawy, zamówień, instrukcji i statusu płatności.
ZACHOWANY MATERIAŁ	Zachowano reklamę i przedstawioną strukturę. Data jest deklarowaną datą eksportu. Nie oznacza zweryfikowanego czasu dostępu, pobrania lub włamania.

ALTERNATYWY	Stara baza zamówień, materiał pośrednika, fikcyjna próbka lub wiele wierszy na klienta pasują do opisu. Etykieta 72K nie ma ustalonego mianownika odrębnych osób.
REAKCJA	Właściwa usługa powinna porównać strukturę z bieżącymi i starszymi systemami oraz dostawcami. Obsługa powinna oczekiwać rozmów przywołujących prawdziwe dostawy. Pole statusu płatności nie dowodzi ujawnienia danych karty.

Wniosek

Nie ustalono autentyczności, aktualności, liczby osób ani danych kart.

4.8 Przypadek D: oferta podróżna z niejasnym mianownikiem kraju (B04)

Karta dowodowa B04 — 11 maj 2026

MDGhost | Forum | Forum | Angielski

ORYGINAŁ

Type: Airline Ticketing & Travel Data Format: csv Records: 10.3M

TŁUMACZENIE

Typ: bilety lotnicze i podróże. Format: csv. Rekordy: 10,3 mln.

Zachowany materiał

Ogłoszenie deklaruje 10,3 miliona rekordów podróżnych powiązanych z pośrednikiem związanym z Polską.

Nie ustalono

Nie ustalono autentyczności, bieżącego dostępu, daty pozyskania ani liczby polskich mieszkańców.

D

PRZYPADEK D

Oferta podróżna z niejasnym mianownikiem kraju

Karta dowodowa B04 | 11 maj 2026 | Forum | Podróże

Niezweryfikowane ogłoszenie

DEKLARACJA	Wpis z 11 maja reklamował 10,3 miliona rekordów podróżnych z polami tożsamości i kontaktu. Powiązane tytuły wątku wspominały też dostęp do panelu. Zachowana treść nie potwierdza tego dostępu.
ZACHOWANY MATERIAŁ	Treść ogłoszenia łączy deklarowany zbiór z pośrednikiem podróżnym związanym z Polską. Podobne sformułowania występują w innych zachowanych wpisach. Uzasadnia to ciągłość reklamy, a nie tożsamość pliku lub niezależnie potwierdzony kolejny incydent.

ALTERNATYWY	Międzynarodowy zbiór rezerwacji, dane strony trzeciej lub starszy materiał mogłyby być reklamowane pod marką pośrednika. Pokazana geografia nie ogranicza się do Polski. Rekordów nie można uznać za polskich mieszkańców.
KONTRTWIERDZENIE	Późniejsza odpowiedź kwestionuje autentyczność i opisuje ofertę jako ponowienie rzekomo fałszywego materiału marcowego. To dowód sporu, a nie niezależna ocena pliku. Raport nie rozstrzyga jednej deklaracji przez przyjęcie drugiej [S1].
REAKCJA	Firmy podróżne powinny ocenić dostawców rezerwacji i zależności zawiadamiania klientów. Wiarygodna wiadomość o podróży nadal wymaga niezależnego sprawdzenia przed zwrotem, zmianą konta lub nową dyspozycją płatniczą.

Wniosek

Nie ustalono autentyczności, bieżącego dostępu, daty pozyskania ani liczby polskich mieszkańców.

4.9 Przypadek E: użytkownicy i wiersze bazy to różne wielkości (B05)

Karta dowodowa B05 — 5 sty 2026

daghetiaw | Forum | Forum | Angielski

ORYGINAŁ

Dump Date : 03/01/2026 - User Registred : 239,434 Lines : 7,456,341

TŁUMACZENIE

Data zrzutu: 03/01/2026. Zarejestrowani użytkownicy: 239 434. Wiersze: 7 456 341.

Zachowany materiał

Wpis deklaruje 239 434 użytkowników i 7 456 341 wierszy. To różne jednostki.

Nie ustalono

Nie ustalono autentyczności, deklarowanej daty, liczby osób ani ekspozycji wszystkich wymienionych pól.

E

PRZYPADEK E

Użytkownicy i wiersze bazy to różne wielkości

Karta dowodowa B05 | 5 sty 2026 | Forum | Usługi konsumenckie

Niezweryfikowane ogłoszenie

DEKLARACJA	Wpis z 5 stycznia reklamował 239 434 zarejestrowanych użytkowników i 7 456 341 wierszy platformy zamówień. Podawał datę zrzutu we własnym formacie oraz pola tożsamości, kontaktu, dostawy i operacji.

ZACHOWANY MATERIAŁ	Zachowano opis i materiał przypominający schemat. Raport nie publikuje danych osobowych ani nie traktuje listy pól jako dowodu ujawnienia. Odpowiedzi i kopie zwiększają widoczność bez potwierdzenia pierwotnego twierdzenia.
ALTERNATYWY	Wiersze mogą obejmować powtarzające się zamówienia, tabele techniczne i konfigurację. Historyczna kopia, zmieniona etykieta lub fikcyjny wyciąg mogą tworzyć takie ogłoszenie. Stosunek użytkowników do wierszy nie daje sensownego szacunku poszkodowanych.
REAKCJA	Usługa powinna porównać strukturę i daty we własnym uprawnionym procesie. Rozdziel konta, tożsamości klientów i wiersze transakcyjne podczas oceny. Komunikat publiczny powinien zachować te jednostki.

Wniosek

Nie ustalono autentyczności, deklarowanej daty, liczby osób ani ekspozycji wszystkich wymienionych pól.

4.10 Przypadek F: powtarzana promocja danych sklepu (B06)

Karta dowodowa B06 — 2 lut 2026

Robert2025 | Forum | Forum | Angielski

ORYGINAŁ

Country: Poland lines: 100K

TŁUMACZENIE

Kraj: Polska. Wiersze: 100K.

Zachowany materiał

Ogłoszenie deklaruje 100K wierszy sklepu. Późniejsze wpisy promują wątek.

Nie ustalono

Nie ustalono autentyczności, aktualności, liczby klientów ani wykonanej transakcji.

F

PRZYPADEK F

Powtarzana promocja danych sklepu

Karta dowodowa B06 | 2 lut 2026 | Forum | Handel

Niezweryfikowane ogłoszenie

DEKLARACJA	Wpis z 2 lutego oferował zbiór polskiego sklepu oznaczony 100K wierszy. Późniejsza aktywność głównie promuje ten sam wątek. Powtórzenie nie jest niezależnym potwierdzeniem.

CO POZOSTAJE NIEZWERYFIKOWANE	Raport nie ustala autentyczności, odrębnych klientów, daty pozyskania ani bieżącego dostępu. Reklamowany pośrednik transakcji nie potwierdza materiału.
ALTERNATYWY	Stara kopia, zdublowane zamówienia, pakiet od pośrednika lub fikcyjne dane pasują do oferty. Ogłoszenie nie rozstrzyga tych możliwości.
REAKCJA	Po pasującym sygnale sklep powinien ocenić eksporty klientów, dostawców i logi. Zapisz, czy dopasowanie dotyczy starego materiału już obsłużonego. Nie przedstawiaj każdej odpowiedzi promocyjnej jako nowego incydentu.

Wniosek

Nie ustalono autentyczności, aktualności, liczby klientów ani wykonanej transakcji.

4.11 Czego zachowane dowody nie łączą

Zachowany zbiór ofert nie ustala związku tych dossier z oficjalnymi przypadkami MyDr, Medyc, FELG, Fakturowni lub Autopay. Podobny sektor nie wystarcza do połączenia. Piętnaście oficjalnych kart w rozdziale 5 pozostaje osobną ścieżką.

Ostatnia oferta gastronomiczna jest bieżącą reklamą z niezweryfikowaną aktualnością danych. Wpis powtarzający historię ePUAP jest wiadomością prasową, a nie dodatkowym dowodem. Potwierdzenie zapewnia własna relacja ministerstwa [S31].

4.12 Dodatkowe oferty i usługi z motywem administracji

Ogłoszenie z 16 listopada wymienia skrzynkę podmiotu publicznego za 550 USD i deklaruje bieżący stan. Zachowana treść nie dowodzi kontroli skrzynki. Alternatywy obejmują fikcyjny stan, odsprzedaż lub usługę podszywania się (B08).

Sierpniowa oferta pocztowa opisuje pola nadawców i odbiorców bez ustalonej liczby lub źródła. Podobne dane może mieć integracja sprzedawcy. Listopadowa oferta przesyłek zawiera przykłady oznaczone jako Polska, bez ustalenia wyłącznie polskiej populacji lub włamania do polskiej organizacji (B09, B11).

Oferta serwisu ogłoszeniowego z 27 kwietnia deklaruje 23 miliony rekordów i cenę 1 980 USD. Skromne pola kontaktowe mogą pochodzić z publicznych ogłoszeń, zestawu leadów, starszych informacji lub fikcji. Nie ustalono skali ani włamania do platformy (B10).

Karta dowodowa B08 — 16 lis 2026

kenpiraa | Forum | Forum | Angielski

ORYGINAŁ

$550 [...] Poland Government mailbox · in stock

TŁUMACZENIE

550 USD [...] skrzynka administracji w Polsce · dostępna.

Uwaga. Pominięcie oznaczono; stan oferty i cena pozostają deklaracjami.

Zachowany materiał
Ogłoszenie wycenia rzekomą skrzynkę podmiotu publicznego na 550 USD i deklaruje bieżący stan.

Nie ustalono
Nie potwierdzono dostępności reklamowanej skrzynki, kontroli nad nią, dostępu ani skuteczności żądań.

Karta dowodowa B09 — 23 sie 2026

updap | Forum | Forum | Angielski

ORYGINAŁ

If you want this base or other (i have many bases)

TŁUMACZENIE

Jeśli chcesz tę bazę lub inną (mam wiele baz).

Zachowany materiał
Wpis deklaruje zbiór nadawców i odbiorców oraz pokazuje strukturę pól.

Nie ustalono
Nie ustalono autentyczności, liczby rekordów, aktualności ani włamania do operatora pocztowego.

Karta dowodowa B10 — 27 kwi 2026

xcgtyrewty | Forum | Forum | Angielski

ORYGINAŁ

Type: Poland Online Marketplace / Classifieds Format: CSV Records: 23M Data: Full Name, Region, Mobile Number Price: 1980 USD

TŁUMACZENIE

Polski serwis ogłoszeniowy. CSV. Rekordy: 23M. Imię i nazwisko, region, telefon. Cena: 1 980 USD.

Zachowany materiał
Ogłoszenie deklaruje 23 miliony rekordów i cenę 1 980 USD.

Nie ustalono
Nie ustalono autentyczności, odrębności osób, pochodzenia, daty ani włamania do platformy.

Karta dowodowa B11 — 13 lis 2026

thisversace | Forum | Forum | Angielski

ORYGINAŁ

tracking1 tracking2 recipient country address state city zip phone created_at content declared_value weight

TŁUMACZENIE

Śledzenie, odbiorca, kraj, adres, region, miasto, kod, telefon, data, zawartość, wartość, waga.

Zachowany materiał
Wpis pokazuje nagłówki danych przesyłek i przykłady oznaczone jako Polska.

Nie ustalono
Nie ustalono autentyczności, aktualności, liczby odbiorców, polskiej wyłączności ani źródła pliku.

To uzupełniające obserwacje reklam. Nie powiększają siedmiu szczegółowych dossier ani liczby oficjalnych incydentów.

4.13 Przypadek U: pliki telekomu i dostęp do pomocy (B12)

Karta dowodowa B12 20 mar 2026

Katarinka | Forum | Forum | Angielski

ORYGINAŁ

POLISH ISP DATABASE+FILES+HELPDESK ACCESS

TŁUMACZENIE

Polska baza ISP, pliki i dostęp do systemu pomocy.

Zachowany materiał
Ogłoszenie deklaruje pliki, wiersze użytkowników, zgłoszenia i dostęp do systemu pomocy telekomu.

Nie ustalono
Nie ustalono autentyczności, aktualności, liczby abonentów ani działającego dostępu.

U

PRZYPADEK U

Pliki telekomu i dostęp do pomocy

Karta dowodowa B12 | 20 mar 2026 | Forum | Telekomunikacja

Niezweryfikowana reklama bazy i dostępu

DEKLARACJA	Ogłoszenie z 20 marca oferuje polską bazę telekomunikacyjną, pliki i dostęp do systemu pomocy. Deklaruje około 29 578 plików, eksport użytkowników z 17 556 wierszami i 51 936 wierszy zgłoszeń. To różne jednostki [S1].
CO ZACHOWANO	Opis wymienia eksporty baz, role systemu obsługi i kategorie załączników. Nagłówki obejmują umowy, faktury, instalacje i pola dokumentów tożsamości. Ustalają treść reklamy, bez weryfikacji plików lub kont.
CO POZOSTAJE NIEZWERYFIKOWANE	Nie ustalono autentyczności, bieżącego dostępu do pomocy, daty pozyskania ani liczby abonentów. Wymienione główne kategorie plików nie uzgadniają całej deklarowanej liczby. Wiersze zgłoszeń mogą powtarzać abonenta albo dotyczyć pracy wewnętrznej.
ALTERNATYWY	Starszy eksport, kopia wykonawcy, połączony zbiór lub fikcyjny wykaz mogą pasować do opisu. Deklarowana rola administracyjna sama nie ustala posiadania działającej sesji.
REAKCJA	Operatorzy powinni sprawdzać eksporty obsługi i repozytoria załączników razem ze zdalną administracją. Dopasuj istotny sygnał do własnego systemu i struktury danych. Sprawdź dostęp, uprawnienia i konkretny zakres danych w autoryzowanym procesie.

Wniosek

Nie ustalono autentyczności, aktualności, liczby abonentów ani działającego dostępu.

4.14 Mniejsze bazy i reklamy uprzywilejowanego dostępu

Kwietniowa reklama bazy strony deklaruje cztery tabele aplikacji z 489 wierszami, w tym sześć wierszy użytkowników. Łączna liczba 9 338 obejmuje też metadane schematu systemowego. Nie należy traktować jej jako liczby klientów; poprawność danych logowania i uprawnienia administratora są niezweryfikowane (B13) [S1].

Wpis pośrednika z 6 kwietnia zawiera dwie anonimowe polskie oferty VPN, związane z budownictwem i edukacją. Reklamuje różne role uprzywilejowane. Nie ustalono bieżącego dostępu ani uprawnień, a wspólna reklama nie dowodzi wspólnego właściciela środowisk (B14) [S1].

Karta dowodowa B13 — 6 kwi 2026

Katarinka | Forum | Forum | Angielski

ORYGINAŁ

Application Tables: 4 Application Rows Total: 489

TŁUMACZENIE

Tabele aplikacji: 4. Łącznie wierszy aplikacji: 489.

Zachowany materiał

Ogłoszenie deklaruje cztery tabele aplikacji z 489 wierszami, w tym sześć wierszy użytkowników.

Nie ustalono

Nie ustalono autentyczności, poprawności danych logowania ani uprawnień; większa suma obejmuje metadane.

Karta dowodowa B14 — 6 kwi 2026

KazeFreak | Forum | Forum | Angielski

ORYGINAŁ

Enterprise Admin privileges. [...] Database Admin (SA) privileges.

TŁUMACZENIE

Uprawnienia Enterprise Admin. [...] Uprawnienia administratora bazy (SA).

Zachowany materiał

Jeden wpis reklamuje dwie anonimowe polskie oferty VPN z różnymi deklarowanymi rolami.

Nie ustalono

Nie ustalono bieżącego dostępu, uprawnień ani związku między środowiskami.

Inne zachowane oferty pokazują ograniczenia dat i pochodzenia. Marcowa reklama sklepu wprost oznacza rzekomy wyciek jako 2025. Duża kompilacja danych logowania przyznaje powtarzanie adresów z różnymi hasłami. Bieżąca data wpisu i duża liczba wierszy nie ustalają nowego włamania do organizacji [S1].

Kwietniowa reklama sprzedaży podatności wskazuje anonimowe polskie cele komercyjne. To deklaracja możliwości sprzedawcy, bez ustalonego wykorzystania, bieżącej kontroli lub skutków. Traktuj ją jako sygnał do sprawdzenia zasobu, a nie dowód zakończonego incydentu [S1].

Wpis z 16 maja o zrzucie strony komercyjnej deklaruje pola danych logowania i nazwisk w załącznikach tekstowych, bez liczby wierszy lub daty pozyskania. Dopuszcza skróty haseł. Nie ustalono zawartości, poprawności ani bieżącego dostępu (B15) [S1].

Karta dowodowa B15 16 maj 2026

org1877 Forum Forum Angielski

ORYGINAŁ

including multiple email and password parts, first and last name, passwords can be hashed*

TŁUMACZENIE

w tym części adresów e-mail i haseł, imię i nazwisko, hasła mogą być skrótami*

Zachowany materiał
Wpis deklaruje zrzut komercyjnej strony i trzy załączniki tekstowe z polami danych logowania i nazwisk.

Nie ustalono
Nie ustalono autentyczności, zawartości załączników, formatu haseł, liczby osób ani bieżącego dostępu.

NAJWAŻNIEJSZE WNIOSKI

01
Rozdzielaj reklamowany dostęp, wielkość i aktualność danych.

02
Podobne wpisy ustalają ciągłość reklamy, a nie tożsamość pliku lub właściciela.

03
Sprawdzaj konta i strukturę przed przyjęciem deklarowanej liczby poszkodowanych.

ROZDZIAŁ 05

Potwierdzone incydenty i zarzuty według sektorów

TEN ROZDZIAŁ ODPOWIADA

Które ujawnienia zmieniają reakcję sektora i jakie niepewności pozostają?

5.1 Decyzje sektorowe 40
5.2 Przypadek G: MyDr i historyczne dane medyczne 41
5.3 Przypadek H: Medyc i granica między dochodzeniem a skalą 42
5.4 Przypadek I: FELG i deklaracje tożsamości sprawcy 43
5.5 Przypadek J: Wyciek kodu poznańskiej uczelni 44
5.6 Przypadek K: zmiana oceny Uniwersytetu Warszawskiego 45
5.7 Przypadek L: odtwarzanie szpitala po ransomware 46
5.8 Przypadek M: enel-med rozdziela opiekę i pytania o dane 47
5.9 Przypadek N: odtwarzanie SOP i kalendarz działalności 48
5.10 Przypadek O: ePUAP i przywracanie etapami 49
5.11 Przypadek P: ostatni incydent dostępu w Autopay 50
5.12 Czego nie można zsumować 50
5.13 Dalsze komunikaty medyczne i przemysłowe 51
5.14 Przypadek Q: firma przemysłowa oddziela szyfrowanie od możliwego kopiowania 51
5.15 Przypadek R: Żabka i konto zewnętrznego dostawcy 52
5.16 Przypadek S: ZUS potwierdza ograniczone zdarzenie dostępności 53
5.17 Przypadek T: kwietniowy komunikat Cyfrowego Polsatu 54
5.18 Inne komunikaty mają węższy zakres 54
5.19 Przypadek V: dostęp do narzędzia poczty i większa oferta danych (B17) 55

15 szczegółowych kart o partiach na źródłach oficjalnych, odrębnych od ofert podziemia

ROZDZIAŁ 05

Potwierdzone incydenty i zarzuty według sektorów

W SKRÓCIE

Oprogramowanie medyczne, księgowość, edukacja i usługi publiczne dostarczają najczytelniejszych oficjalnych opisów. Część komunikatów potwierdza kopiowanie danych; inne potwierdzają dostęp, pozostawiając kopiowanie niewyjaśnione. Incydenty dostępności w ochronie zdrowia tworzą osobny problem odtwarzania. Poniższe przypadki zachowują te różnice i nie tworzą krajowej liczby poszkodowanych. Zacznij od zakresu własnego konta i dostawcy, a następnie wybierz właściwą reakcję dotyczącą prywatności, tożsamości i ciągłości.

5.1 Decyzje sektorowe

Tabela kieruje dowody do pierwszego odpowiedzialnego zespołu. Obecność sektora nie mierzy jego udziału w krajowej liczbie incydentów.

Sektor	Obserwacja lub relacja	Rodzaj dowodu	Pierwsza reakcja
Oprogramowanie medyczne	Historyczne rekordy MyDr; dochodzenie Medyc; dostęp do danych pacjentów FELG [S5][S7][S8]	Oficjalne komunikaty o różnym zakresie i pewności	Uzyskaj informacje dla gabinetu i zachowaj ocenę ryzyka administratora
Świadczenia medyczne	Dostęp do danych enel-med; ransomware w szpitalu regionalnym [S12][S35]	Relacje dostawcy i organu sektorowego	Oddziel komunikację z pacjentami od ciągłości klinicznej i odtwarzania
Oprogramowanie biznesowe	Fakturownia potwierdza kopiowanie informacji o kontach, kontrahentach i fakturach [S10]	Potwierdzenie firmy	Zmień właściwe dane dostępowe i niezależnie potwierdzaj zmiany płatnicze
Edukacja	Uczelnia potwierdza kopiowanie i późniejszą publikację; nie ustalono wszystkich osób [S41]	Potwierdzenie uczelni	Oceń użycie poprawnych danych logowania i dostęp do repozytoriów wydziałowych
Usługi publiczne	Ograniczenia SOP i etapowe przywracanie ePUAP [S31] [S33][S34]	Oficjalne ujawnienia	Utrzymuj alternatywne procesy i komunikaty oparte na faktach
Płatności	Autopay potwierdza dostęp; kopiowanie i użycie pozostają niepotwierdzone [S45]	Potwierdzenie firmy z wyraźnymi ograniczeniami	Stosuj indywidualne zalecenia i monitoruj nieautoryzowane transakcje

Sektor	Obserwacja lub relacja	Rodzaj dowodu	Pierwsza reakcja
Przemysł i usługi	Polskie wpisy na stronach wymuszeń w różnych kategoriach branżowych [S3]	Twierdzenia przestępcze	Sprawdź pasujący zarzut i niezależnie przetestuj odtwarzanie
Energia i badania	Historyczny raport energetyczny i zatrzymana próba wobec instytutu [S18][S43]	Relacje oficjalne, różne daty i wyniki	Oceń zdalne zarządzanie i bezpieczną ciągłość procesów

5.2 Przypadek G: MyDr i historyczne dane medyczne

PRZYPADEK G

G

MyDr i historyczne dane medyczne

Oprogramowanie medyczne

Oficjalna relacja dostępu; możliwa populacja

RELACJA OFICJALNA	Ministerstwo poinformowało 12 sierpnia, że firma potwierdziła nieuprawniony dostęp do historycznych danych gabinetów do kwietnia 2024. Incydent mógł dotyczyć 18,8 miliona osób i ponad 12 000 placówek [S5].
CHRONOLOGIA	Sierpniowe ujawnienie dotyczyło starszych rekordów. UODO opublikował w tym okresie wyjaśnienia dla administratorów. Później opisywał skargi i zgłoszenia administratorów, lecz są to inne jednostki niż potencjalnie objęte osoby [S6][S7].
CO USTALONO	Ministerstwo przekazało potwierdzenie firmy dotyczące nieuprawnionego dostępu. Ten sam komunikat wskazywał brak zakłóceń bieżącej opieki i wystawiania recept. Działająca usługa nie rozstrzygała więc kwestii poufności.
CO POZOSTAJE NIEUSTALONE	Potencjalna populacja nie jest zweryfikowaną przez autorów liczbą odrębnych osób. Nie można założyć, że późniejsza oferta przestępcza zawiera całą tę populację lub wynika z tego samego dostępu.
ALTERNATYWY DO SPRAWDZENIA	Oferowana próbka może być stara, częściowa, połączona z innym źródłem lub błędnie opisana. Dopasowanie rekordów powinien ocenić odpowiedzialny administrator w uprawnionym procesie reagowania.
REAKCJA	Gabinety powinny uzyskać własny zakres od procesora i ocenić obowiązki zawiadomienia. Obsługa pacjentów powinna jasno wyjaśniać sytuację i nie prosić o przekazywanie wrażliwych dokumentów przez niezweryfikowany kontakt.

Wniosek

Uzyskaj zakres gabinetu przed przyjęciem całej populacji.

5.3 Przypadek H: Medyc i granica między dochodzeniem a skalą

PRZYPADEK H

H

Medyc i granica między dochodzeniem a skalą

Oprogramowanie medyczne

Dochodzenie organu: skala niezweryfikowana

RELACJA OFICJALNA	Komunikat UODO z 25 września opisuje działania CBZC dotyczące Medyc i planowaną kontrolę Qbusoft. Możliwą liczbę pięciu milionów osób przypisuje doniesieniom medialnym [S7].
CO USTALONO	Organ publicznie odniósł się do incydentu i dostawcy. Komunikat dowodzi oficjalnej reakcji, a nie niezależnego potwierdzenia rozmiaru zbioru podawanego w ogłoszeniach lub mediach.
CO POZOSTAJE NIEUSTALONE	Raport nie ustala ostatecznej liczby odrębnych osób ani kopiowania dokumentacji medycznej każdego użytkownika. Placówki mogą przechowywać różne informacje i otrzymywać różne oceny zakresu.
ALTERNATYWY I OGRANICZENIA	Zarzut dotyczący centralnej platformy może obejmować jednego klienta, część tabel lub szerszy zbiór. Samo ogłoszenie nie pozwala rozstrzygnąć tych możliwości. Powtarzanie liczby w mediach nie jest nowym pomiarem.
REAKCJA	Gabinet korzystający z oprogramowania powinien poprosić o opis dotyczący jego konta i zachować własną chronologię stwierdzenia naruszenia. Komunikaty publiczne powinny odróżniać potwierdzone kategorie danych od tych nadal badanych.

Wniosek

Dochodzenie i szacunek mediów to odrębne dowody.

5.4 Przypadek I: FELG i deklaracje tożsamości sprawcy

PRZYPADEK I

FELG i deklaracje tożsamości sprawcy

Oprogramowanie medyczne

Dostawca potwierdza dostęp

RELACJA OFICJALNA	Komunikat FELG z 1 października potwierdza dostęp do danych pacjentów i opisuje żądanie okupu. Wskazany udział 10% przypisuje osobie deklarującej odpowiedzialność. Nie przedstawia tej wartości jako własnego zakończonego ustalenia [S8].
CHRONOLOGIA	Późniejsza aktualizacja umieszcza reakcję na otrzymane zgłoszenie 29 września. Aktualizacja z 7 października mówi o ustaleniu objętych placówek i rozpoczęciu indywidualnego informowania. Sekwencja odróżnia otrzymanie zgłoszenia, analizę i zawiadomienie konkretnego klienta.
CO POZOSTAJE NIEUSTALONE	Komunikat opisuje osobę podającą się za członka grupy. Biuletyn AHA wskazuje alias i odróżnia sprawcę od wcześniejszych incydentów medycznych. Żadna relacja nie dostarcza autorom zweryfikowanego dowodu wspólnego operatora [S8][S9].
ALTERNATYWY I OGRANICZENIA	Alias może być prawdziwy, zapożyczony lub mylący. Próbka i żądanie okupu nie dowodzą deklarowanego udziału bazy ani sprzedaży. Przypadek nie służy do łączenia incydentów medycznych w jedną organizację przestępczą.
REAKCJA	Gabinet powinien wykorzystać indywidualny zakres od procesora i przeprowadzić własną ocenę administratora. Ogólne zalecenie dostawcy nie zastępuje decyzji administratora wymaganej prawem.

Wniosek

Deklaracja przynależności nie ustala wspólnego operatora.

5.5 Przypadek J: Fakturownia i późniejsze oszustwa płatnicze

J

PRZYPADEK J

Fakturownia i późniejsze oszustwa płatnicze

Oprogramowanie biznesowe

Firma potwierdza kopiowanie

RELACJA OFICJALNA	Firma podaje, że nieuprawniony dostęp trwał 27–28 września i dane skopiowano. Rozszerzony komunikat odróżnia informacje o kontach, materiałach integracyjnych, kontrahentach i fakturach, z różnymi zakresami dat [S10].
CO USTALONO	To potwierdzony incydent poufności. Dostawca odróżnia także dane administrowane przez siebie od danych przetwarzanych dla klientów. Zakresu nie można sprowadzić do twierdzenia, że pobrano wszystkie stare faktury albo wszystkie nowe informacje.
CO POZOSTAJE NIEUSTALONE	Nie określono tutaj wspólnej liczby poszkodowanych. Firma twierdzi, że nie przechowywała danych kart płatniczych ani danych logowania do banków. Informacje płatnicze nie oznaczają więc automatycznie danych kart lub haseł bankowych.
ALTERNATYWY I OGRANICZENIA	Wiarygodne oszustwo fakturowe po komunikacie mogłoby korzystać z tego incydentu, innego ujawnienia lub prawidłowej korespondencji. Dostępność rzeczywistych danych faktury sama nie dowodzi skutecznego oszustwa.
REAKCJA	Klienci powinni wykonać właściwe zmiany dostępu wskazane przez dostawcę i niezależnie sprawdzać nietypowe dyspozycje. Finanse powinny dzwonić do osoby znanej przed żądaniem. Bezpieczeństwo i prywatność powinny zachować ocenę dotyczącą klienta.

Wniosek

Sprawdzaj wrażliwe dyspozycje ze znanym wcześniej kontaktem.

5.6 Przypadek K: zmiana oceny Uniwersytetu Warszawskiego

PRZYPADEK K

K

Zmiana oceny Uniwersytetu Warszawskiego

Edukacja

Uczelnia potwierdza kopiowanie i publikację

RELACJA OFICJALNA	Uczelnia podaje wykrycie dostępu 9 lutego. Późniejszy komunikat wskazuje możliwe kopiowanie w styczniu–lutym i publikację w nocy 15–16 kwietnia [S41].
CO USTALONO	Późniejsza relacja potwierdza kopiowanie i publikację. Opisuje użycie poprawnych danych logowania, najprawdopodobniej uzyskanych przez złośliwe oprogramowanie na urządzeniu użytkownika. Uczelnia przedstawia to pochodzenie jako najbardziej prawdopodobne wyjaśnienie, a nie ustalenie niezależnie odtworzone przez autorów.
ZNACZENIE JEDNOSTEK	Opublikowany zbiór obejmował około 200 000 plików i 850 GB. Około 650 GB stanowiły publiczne materiały audiowizualne. Około 32 800 plików mogło zawierać dane osobowe. To liczby plików i rozmiary, a nie liczba poszkodowanych.
CO POZOSTAJE NIEUSTALONE	Uczelnia nie wskazała w komunikacie każdej objętej osoby. Podała brak zakłóceń lub szyfrowania kluczowych systemów. Brak szyfrowania nie oznaczał braku naruszenia poufności.
REAKCJA	Uczelnie powinny łącznie badać dostęp przez poprawne konta i repozytoria wydziałowe. Rejestr incydentu powinien zachowywać zastąpione oceny wraz z uzasadnieniem zmiany. Lutowy komunikat nie powinien przesłaniać późniejszego, bardziej szczegółowego ujawnienia.

Wniosek

Liczba plików nie jest liczbą poszkodowanych.

5.7 Przypadek L: odtwarzanie szpitala po ransomware

L

PRZYPADEK L

Odtwarzanie szpitala po ransomware

Ochrona zdrowia

Oficjalne szyfrowanie i odtwarzanie

RELACJA OFICJALNA	Artykuł organu sektorowego z 25 marca opisuje ransomware z 8 marca w szpitalu regionalnym. Zaszyfrowano część zasobów, ograniczono dostęp do informacji i wprowadzono tryb pracy awaryjnej [S35].
CO USTALONO	Rzecznik placówki opisuje zakłócenia i przewidywany powrót do równowagi trwający tygodnie. Relacja wyraźnie nie oznacza całkowitego paraliżu. Pomoc na miejscu i zdalnie zapewniało kilka zespołów krajowych i sektorowych.
CO POZOSTAJE NIEUSTALONE	Artykuł wskazuje ryzyko poufności, lecz nie podaje ostatecznej liczby danych wyprowadzonych lub osób. Nie uzasadnia przypisania zdarzenia określonej grupie wymuszającej okup bez dodatkowych dowodów.
REAKCJA	Szpitale powinny testować pracę kliniczną przy ograniczonym dostępie do danych. Test odtworzenia powinien obejmować bieżącą opiekę, bezpieczny zapis ręczny, uzgodnienie dokumentacji i akceptację biznesową. Sam sukces zadania kopii nie wykazuje tych zdolności.

Wniosek

Zaakceptuj odtworzenie po sprawdzeniu procesu klinicznego.

5.8 Przypadek M: enel-med rozdziela opiekę i pytania o dane

PRZYPADEK M

M

Enel-med rozdziela opiekę i pytania o dane

Ochrona zdrowia

Dostęp potwierdzony; zakres szacowany

RELACJA OFICJALNA	Komunikat z 27 września podaje wykrycie dostępu do części infrastruktury i danych pacjentów 24 września. Według dostawcy incydent mógł dotyczyć około 3% bazy pacjentów [S12].
CO USTALONO	Dostawca potwierdza dostęp i indywidualne zawiadomienia. Podaje też normalne działanie placówek. Procent jest jego szacunkiem, bez mianownika pozwalającego przeliczyć go na liczbę osób.
CO POZOSTAJE NIEUSTALONE	Raport nie zakłada objęcia wszystkich pacjentów, każdej kategorii danych lub wszystkich systemów. Nie łączy zdarzenia z innym incydentem medycznym wyłącznie z powodu bliskości czasu.
REAKCJA	Korzystaj z indywidualnych zawiadomień i sprawdzonych kontaktów dostawcy. Przygotuj personel na oszustów podających prawdziwe dane pacjentów, zachowując rozróżnienie między ciągłością opieki a badaniem danych.

Wniosek

Działająca opieka i badanie poufności mogą współistnieć.

5.9 Przypadek N: odtwarzanie SOP i kalendarz działalności

PRZYPADEK N

N

Odtwarzanie SOP i kalendarz działalności

Administracja

Oficjalny incydent: zakres danych badany

RELACJA OFICJALNA	Ministerstwo Kultury opisuje incydent z 6 października w Systemie Obsługi Programów. Komunikat z 9 października mówi o izolacji systemu i możliwym dostępie do danych użytkowników; zakres nadal badano [S33].
CHRONOLOGIA	Ministerstwo 28 października powiązało opóźnienie naborów na 2027 z odtwarzaniem. Podało przywrócenie z kopii danych wprowadzonych do 5 października. Przywrócenie danych i pełnej usługi to dwa odrębne ustalenia [S34].
CO POZOSTAJE NIEUSTALONE	Liczba zarejestrowanych użytkowników nie oznacza liczby osób, których dane skopiowano. Komunikat nie przypisuje zdarzenia państwu, grupie ani ogłoszeniu na rynku przestępczym.
REAKCJA	Publiczne i prywatne systemy dotacyjne powinny zachowywać dowody złożenia dokumentów i wyjaśniać zmiany obsługi. Odbiór odtworzenia musi obejmować rzeczywiste składanie wniosków i terminy, a nie tylko przywrócenie bazy.

Wniosek

Przywróć obsługę wniosku i dowody jego złożenia.

5.10 Przypadek O: ePUAP i przywracanie etapami

PRZYPADEK O

EPUAP i przywracanie etapami

Administracja

Oficjalne przywracanie etapami

RELACJA OFICJALNA	Ministerstwo Cyfryzacji ogłosiło 19 listopada pełne przywrócenie po incydencie wykrytym 10 listopada. Opisało ograniczenia zapobiegawcze, analizę, dodatkowe zabezpieczenia i testowanie elementów przed udostępnieniem [S31].
CHRONOLOGIA	Ten sam komunikat wskazuje rozwiązanie przejściowe 15 listopada oraz działanie wszystkich usług transakcyjnych przez wskazany portal usług publicznych 16 listopada. Pełne działanie ePUAP przywrócono 19 listopada.
CO POZOSTAJE NIEUSTALONE	Komunikat nie ustala metody ataku, sprawcy ani liczby skradzionych danych osobowych. Podaje też brak śladów rozszerzenia poza zidentyfikowany obszar. To wynik przedstawiony przez ministerstwo w granicach jego analizy.
REAKCJA	Organizacje zależne od elektronicznych pism powinny testować dopuszczoną alternatywę i zachowywać dowody prób oraz wykonania. Komunikacja powinna odróżniać ograniczony dostęp, częściowe przywrócenie i pełne działanie.

Wniosek

Oddziel częściowe przywrócenie od pełnej usługi.

5.11 Przypadek P: ostatni incydent dostępu w Autopay

P

PRZYPADEK P

Ostatni incydent dostępu w Autopay

Płatności

Dostęp potwierdzony; kopiowanie nieustalone

RELACJA OFICJALNA	Autopay podaje wykrycie nieautoryzowanego dostępu do infrastruktury i części informacji o przetworzonych płatnościach 11 listopada. Kopiowania i użycia danych nie potwierdzono, ale firma nie może ich wykluczyć [S45].
CO USTALONO	Dostawca zablokował dostęp i opisuje bezpośrednią komunikację z potencjalnie objętymi klientami. PRNews relacjonował komunikat w tym samym ostatnim okresie. Wykorzystane źródła nie podają liczby osób [S46].
ALTERNATYWY I OGRANICZENIA	Dostęp, kopiowanie i późniejsze wykorzystanie to odrębne twierdzenia. Ogłoszenie sprawcy ani podsumowanie w mediach społecznościowych nie powinno usuwać niepewności firmy. Raport nie wywodzi z tego utraty danych kart.
REAKCJA	Klienci powinni stosować sprawdzone zalecenia dotyczące ich konta i zgłaszać nieautoryzowane transakcje ustaloną drogą bankową. Obsługa powinna oczekiwać oszustów powołujących się na prawdziwy incydent przy żądaniu kodów lub pilnego działania.

Wniosek

Korzystaj z indywidualnych zawiadomień i ustalonych kanałów bankowych.

5.12 Czego nie można zsumować

Piętnaście szczegółowych przypadków to dossier o różnych dowodach i jednostkach. Nie oznaczają piętnastu zdarzeń o równej wadze ani pełnej liczby krajowej. Część dotyczy dostępu bez ustalonej populacji; inne ciągłości bez opublikowanego potwierdzenia kradzieży danych.

Raport nie dodaje szacunków pacjentów, plików uczelni, kont platform i wpisów ransomware. Osoby mogą występować u kilku dostawców. Kolejne komunikaty mogą też opisywać etapy tego samego zdarzenia.

5.13 Dalsze komunikaty medyczne i przemysłowe

Trzy dodatkowe marcowe komunikaty medyczne opisują szyfrowanie lub niedostępność dokumentacji. Jeden dostawca wykrył ransomware 13 marca, drugi opisuje zdarzenie 24 marca, a podmiot rehabilitacyjny wykrył je 31 marca. Wypowiedzi zachowują zastrzeżenia dotyczące możliwego lub prawdopodobnego pozyskania danych [S56][S57][S58].

Komunikat dotyczący 24 marca opisuje odzyskanie dostępu do dokumentacji wytworzonej do 24 czerwca 2021. Nie dowodzi to trwałej utraty nowszych rekordów. Sąsiadujące historyczne zawiadomienie o dokumentacji papierowej innego dostawcy również wyłączono z tegorocznego ransomware.

Na początku listopada oficjalne ostrzeżenie sanitarne objęło Polskę kampanią wobec sterowania chłodzeniem. PAP przytoczyła potwierdzenie jednego polskiego urządzenia przez szefa CERT, bez straty materialnej po interwencji operatora. Szersza populacja urządzeń odsłoniętych jest inną miarą [S54][S55].

Komunikaty dodają konkretne wnioski o ciągłości i sterowaniu przemysłowym. Pozostają wzmiankami, a nie dodatkowymi szczegółowymi kartami. Raport nie przypisuje operatora państwu lub grupie przestępczej.

5.14 Przypadek Q: firma przemysłowa oddziela szyfrowanie od możliwego kopiowania

PRZYPADEK Q

Firma przemysłowa oddziela szyfrowanie od możliwego kopiowania

Przemysł

Szyfrowanie potwierdzone; kopiowanie nieustalone

RELACJA OFICJALNA	Firma przemysłowa podaje, że wykryła ransomware 29 października, a możliwy początek przypadał na 28 października. Potwierdza zaszyfrowanie części danych i utratę dostępu. Kopiowanie i publikacja pozostają niepotwierdzone [S71].
CHRONOLOGIA	Historia komunikatu wskazuje pierwszą publikację 3 listopada i rozszerzoną aktualizację 19 listopada. Nagłówek podaje 10 listopada. To daty strony informacyjnej, a nie trzy odrębne ataki.
CO POZOSTAJE NIEUSTALONE	Firma nadal ustalała zakres danych, osób i okresów. Wskazane przez nią ryzyko dostępu nie daje zweryfikowanej liczby osób ani dowodu sprzedaży.
REAKCJA	Wybierz komunikat właściwy dla danej relacji i niezależnie sprawdzaj nietypowe dyspozycje. Zespoły odtwarzania i prywatności powinny osobno śle-

dzić odzyskanie dostępu, integralność danych, możliwe kopiowanie i indywidualne zawiadomienia.

Wniosek

Osobno śledź integralność, przywracanie dostępu i zakres prywatności.

5.15 Przypadek R: Żabka i konto zewnętrznego dostawcy

R

PRZYPADEK R

Żabka i konto zewnętrznego dostawcy

Handel

Potwierdzony dostęp przez konto dostawcy

RELACJA OFICJALNA	Oświadczenie Żabki z 4 sierpnia potwierdza nieuprawniony dostęp przez konto zewnętrznego dostawcy. Dotyczy wybranych zasobów technicznych wspierających wymianę informacji między franczyzodawcą a franczyzobiorcami. Firma podaje, że wykryła dostęp pod koniec poprzedniego tygodnia i go zablokowała [S72].
CO USTALONO	Firma wskazała konkretną drogę przez konto dostawcy. Podała, że dane transakcyjne, usługi konsumenckie, poufność Żappki i działalność operacyjna pozostały nienaruszone. Nie potwierdza to każdej osobnej deklaracji sprzedawcy o plikach technicznych i repozytoriach.
CO POZOSTAJE NIEUSTALONE	Raport nie ustala liczby osób, sprzedaży ani zgodności każdego reklamowanego obiektu z zakresem oficjalnym. Liczb zasobów technicznych nie należy przedstawiać jako liczby klientów.
REAKCJA	Sprawdź tożsamości dostawców, dozwolone zasoby i awaryjne cofanie uprawnień. Właściciel usługi powinien sprawdzić, czy usunięcie dostępu obejmuje tokeny, sesje i aplikacje delegowane. Zachowaj odrębne ustalenia dotyczące dostawcy, bez założenia udziału każdej usługi konsumenckiej.

Wniosek

Sprawdź tożsamości dostawców, sesje i awaryjne cofanie dostępu.

5.16 Przypadek S: ZUS potwierdza ograniczone zdarzenie dostępności

S

PRZYPADEK S

ZUS potwierdza ograniczone zdarzenie dostępności

Usługi publiczne

Potwierdzony incydent dostępności DDoS

RELACJA OFICJALNA	Komunikat ZUS z 10 sierpnia opisuje przedpołudniowy atak wolumetryczny DDoS na stronę, który mógł też utrudniać dostęp do eZUS. Ogłasza przywrócenie logowania. Wprost podaje, że dane ZUS i klientów nie były zagrożone [S73].
CO POZOSTAJE NIEUSTALONE	Komunikat nie przypisuje sprawcy, nie podaje dokładnego czasu utrudnień ani strat biznesowych. Opisu dostępności nie należy zmieniać w opis kradzieży danych osobowych.
REAKCJA	Właściciele usług publicznych powinni przetestować decyzję o ochronie zewnętrznej, alternatywy dla klienta i rzeczywiste logowanie. Komunikacja powinna wskazywać ograniczony wpływ na usługę oraz dowody wspierające stwierdzenia o danych.

Wniosek

Przetestuj odtworzenie usługi i zachowaj granicę wpływu na dane.

5.17 Przypadek T: kwietniowy komunikat Cyfrowego Polsatu

T

PRZYPADEK T

Kwietniowy komunikat Cyfrowego Polsatu

Telekomunikacja

Potwierdzony kwietniowy dostęp do danych

RELACJA OFICJALNA	Komunikat Cyfrowego Polsatu wprost uzupełnia informację z 29 kwietnia 2026. Dotyczy nieuprawnionego dostępu do części danych klientów w kwietniu. Firma podaje, że monitoring nie wykrył publikacji [S74].
CO USTALONO	Komunikat wymienia możliwe kategorie danych identyfikacyjnych i kontaktowych. Podaje, że nie przełamano zabezpieczeń technicznych, oraz wyklucza loginy, hasła klientów i dane kart. Charakterystyka mechanizmu dostępu pozostaje relacją firmy.
CO POZOSTAJE NIEUSTALONE	Raport nie ustala ogólnej liczby osób. Osobnej oferty dostępu do portalu nie łączy się z tym zdarzeniem bez dowodów. Data odczytu aktualizowanej strony nie jest datą nowego incydentu.
REAKCJA	Obsługa klienta powinna oddzielać ryzyka danych identyfikacyjnych od incydentów haseł i kart. Korzystaj ze zweryfikowanych zaleceń firmy i zakresu danej osoby. Znajomość danych tożsamości nie upoważnia do wrażliwej zmiany konta.

Wniosek

Stosuj zakres danej osoby i zweryfikowane zalecenia ochrony tożsamości.

5.18 Inne komunikaty mają węższy zakres

Komunikat szpitala uniwersyteckiego z 10 marca dotyczy dostępu do skrzynki pracownika wykrytego 2 marca. Korespondencja obejmowała informacje o pacjentach, natomiast wykorzystanie i publikacja były niepotwierdzone. Nie ustalono przerwy w usługach ani liczby osób [S78].

Osobny szpital opisuje wewnętrzny błąd kontroli dostępu z 27 lutego: pracownik zostawił nieupoważnionego byłego pracownika przy zalogowanej stacji. Komunikat nie ustala przeglądania dokumentacji. To przykład prywatności i kontroli dostępu, a nie potwierdzony zdalny cyberatak [S79].

Marcowy komunikat operatora obiektów handlowych potwierdza dostęp i ślady pobrania ograniczonej części plików. Widoczna data to 10 marca, a metadane wskazują 11 marca. Żadna nie ustala początku dostępu. Zakres wymaga oceny danej relacji [S80].

Podpisany 4 listopada komunikat operatora rekreacyjnego potwierdza kilkuminutowy nieuprawniony podgląd kamer 22 października, wykryty 28 października. Nie stwierdza dostępu do sieci lokalnej ani innych danych klientów i nie wskazuje dowodu pobrania obrazów. Ten ograniczony przypadek nie ustala szerszej inwigilacji [S81].

Administrator medyczny osobno opisuje skutki incydentu u niewskazanego dostawcy oprogramowania w sierpniu i wrześniu. Oddziela potwierdzone skutki dla poufności, wysoce prawdopodobną kradzież plików i nieustalone kategorie. Nie identyfikuje dostawcy ani nie ustala ciągłego dostępu jednego sprawcy [S77].

Wrześniowa relacja nadawcy publicznego przytacza oświadczenie pośrednika turystycznego o dostępie do danych klientów, w tym danych tożsamości i dokumentów podróży. Nie odnaleziono osobnego komunikatu pierwotnego. To relacja z zastrzeżeniem, bez utożsamiania jej z reklamą danych podróżnych w podziemiu [S76].

5.19 Przypadek V: dostęp do narzędzia poczty i większa oferta danych (B17)

Karta dowodowa B17 23 sty 2026

Spirigatito Forum Forum Angielski

ORYGINAŁ

487 837 unique users

TŁUMACZENIE

487 837 unikalnych użytkowników

Zachowany materiał

Sprzedawca deklaruje 1 528 945 wierszy, w tym zgłoszenia, i 487 837 unikalnych użytkowników; zachowano schematy kontaktów i wiadomości obsługi.

Nie ustalono

Nie zweryfikowano reklamowanych plików, sum, daty pozyskania ani związku z oficjalnym komunikatem narzędzia poczty.

PRZYPADEK V

V

Dostęp do narzędzia poczty i większa oferta danych

Karta dowodowa B17 | 23 sty 2026 | Forum | Obsługa klientów handlu

Oficjalny komunikat poczty: sumy oferty niezweryfikowane

DEKLAROWANY ZAKRES	Dwa ogłoszenia forumowe z 23 stycznia deklarują 1 528 945 wierszy, w tym zgłoszenia pomocy, oraz 487 837 unikalnych użytkowników związanych z polską firmą handlową. To jednostki sprzedawcy, a nie zweryfikowane osoby. Opisują jedną ofertę, bez ustalenia odrębnych włamań [S1].
OFICJALNY ZAKRES	Firma zgłasza wykrycie dostępu do adresów e-mail korespondentów 23 stycznia. Aktualizacja z 13 lutego ogranicza incydent do narzędzia obsługi poczty i wyklucza dane sklepu internetowego, zamówień oraz płatności [S89].

CO ZACHOWANO	Ogłoszenia zawierają schematy kontaktów i wiadomości obsługi oraz przykłady, których wartości osobowe pominięto. Późniejsza odpowiedź mówi o potwierdzeniu incydentu. Komunikat firmy wspiera węższe zdarzenie dostępu, bez weryfikacji reklamowanych plików lub sum.
CO POZOSTAJE NIEZWERYFIKOWANE	Nie ustalono sum wierszy i użytkowników, autentyczności reklamowanych plików, daty pozyskania ani odrębnych osób. Raport nie ustala, czy oferowana baza jest materiałem opisanym w oficjalnym komunikacie.
REAKCJA	Sprawdź dostęp do poczty i systemu obsługi z właścicielami tożsamości i prywatności. Oceń nietypowe eksporty, zmiany kont i nadużycia prawdziwych szczegółów zgłoszeń. Zweryfikuj zakres przed przyjęciem liczby klientów lub wykonaniem dyspozycji pod pozorem obsługi.
	> [!TAKEAWAY] Potwierdzony dostęp może pozostawiać nieustalone kopiowanie i liczbę osób. ;; Odtwarzanie musi przywrócić proces biznesowy, a nie wyłącznie bazę. ;; Korzystaj z najnowszej szczegółowej relacji oficjalnej, zachowując wcześniejszą chronologię.

Wniosek

Zachowaj odrębny zakres oficjalnego dostępu i deklarowanych sum bazy.

ROZDZIAŁ 06

Haktywizm, DDoS i ostatnia aktywność

TEN ROZDZIAŁ ODPOWIADA

Co odróżnia deklarację polityczną od ustalonego zdarzenia dotyczącego usługi?

9–22 listopada

ostatni okres aktywności w ramach całego roku

6.1 Deklaracje DDoS wymagają własnych dowodów 58
6.2 Deklaracja a relacje źródłowe 58
6.3 Chronologia deklaracji, kampanii i komunikatów 59
6.4 Ostatnia aktywność: 9–22 listopada 60
6.5 Komunikacja zachowująca niepewność 61

ROZDZIAŁ 06

Haktywizm, DDoS i ostatnia aktywność

W SKRÓCIE

Politycznie przedstawiane deklaracje DDoS to jedna ścieżka dowodowa. Oficjalne listopadowe komunikaty o usługach publicznych i płatnościach to inna. Komunikat o odtworzeniu ePUAP nie wskazuje grupy DDoS ani nie potwierdza kradzieży danych. Autopay potwierdza dostęp, pozostawiając kopiowanie niewyjaśnione. Zbieraj pomiary dostępności, utrzymuj zaufany kanał statusowy i oceniaj konkretny incydent przed łączeniem deklaracji ze zdarzeniami.

6.1 Deklaracje DDoS wymagają własnych dowodów

ZeroFox opisuje zaobserwowane 12 stycznia deklaracje NoName057(16) i DarkStorm Team dotyczące polskich organizacji. Badacz przedstawia grupy i ich narrację polityczną. Raport przypisuje te opisy ZeroFox [S30].

Obserwacja ustala publikację deklaracji. Lista celów, zrzut ekranu lub zewnętrzny test dostępności nie ustalają długości, zasięgu geograficznego ani wpływu przerwy na działalność. Nie dowodzą także kierowania przez państwo.

Odniesienia do kraju oraz wypowiedzi o Ukrainie, Rosji lub Białorusi nie powinny stawać się wyjaśnieniem przyjętym przez wydawcę. Uzasadnienie grupy pozostaje jej relacją. Obrońcy mogą potraktować wskazanie celu jako sygnał gotowości bez przyjmowania narracji.

Energetyka24 przytacza oświadczenie podmiotu sektora energii o krótkiej przerwie działania strony i braku zgłoszonego wpływu na usługi operacyjne [S75]. Osobny komunikat pierwotny nie był dostępny do weryfikacji. Ta relacja nie ustala kierowania przez państwo.

6.2 Deklaracja a relacje źródłowe

Panel dotyczy wyłącznie styczniowych deklaracji. Nie łączy ich z listopadowymi incydentami.

Kwestia	Deklaracja sprawcy	Relacja oficjalna	Publiczne badanie
Aktywność	DDoS wobec polskich organizacji według relacji badacza	Nie ustalono tutaj oficjalnego potwierdzenia dla konkretnego celu	ZeroFox opisuje obserwację deklaracji 12 stycznia [S30]
Wpływ	Deklarowana przerwa	Brak uzasadnionej miary czasu i straty biznesowej	Publikacja deklaracji nie jest niezależną telemetrią usługi
Przypisanie	Nazwy grup przy ogłoszeniach	Panel nie ustala przypisania państwu	Orientacja polityczna jest opisem ZeroFox, a nie wnioskiem z języka
Decyzja obrońcy	Sprawdź wskazaną usługę	Uzyskaj fakty od operatora	Zachowaj osobno czas deklaracji, pomiary dostawcy i decyzje

Brak oficjalnego dopasowania nie dowodzi fałszywości deklaracji. Wyznacza granicę wiedzy raportu. Publiczna aktualizacja powinna wyjaśniać ustalenia organizacji, zamiast powtarzać ocenę wpływu podaną przez grupę.

Zachowany wpis NoName057(16) z 13 września także deklaruje aktywność wobec usług publicznych i komercyjnych. Lista celów i odnośniki dostępności nie ustalają zweryfikowanych przerw (B07) [S1].

Karta dowodowa B07 13 wrz 2026

NoName057(16) Kanał Telegram Telegram Angielski

ORYGINAŁ

Poland [...]

TŁUMACZENIE

Polska [...]

Uwaga. Pominięto listę celów i retorykę. Cytowano tylko odniesienie do kraju.

Zachowany materiał
Zachowano deklarację aktywności wobec polskich usług publicznych i komercyjnych.

Nie ustalono
Nie ustalono przerw, czasu, wpływu, ruchu ataku ani odpowiedzialności poza nazwą wyświetlaną.

6.3 Chronologia deklaracji, kampanii i komunikatów

Daty dotyczą zdarzenia lub publikacji wskazanej w wierszu. Urzędowa aktualizacja nie oznacza automatycznie nowego incydentu.

12 sty 2026 **Publiczne badanie**
ZeroFox obserwuje deklaracje NoName057(16) i DarkStorm Team dotyczące polskich organizacji [S30]

12 cze 2026	**CERT Polska** Opisuje phishing Gmail przypisywany UNC1151/Ghostwriter, aktywny od marca [S14]
23 wrz 2026	**CERT Polska** Publikuje analizę mobilnego toll fraud skierowanego do Polski [S15]
10 lis 2026	**Ministerstwo Cyfryzacji** Data incydentu podana później dla ograniczeń ePUAP [S31]
11 lis 2026	**Dostawca płatności** Autopay wykrywa nieautoryzowany dostęp; kopiowanie pozostaje niepotwierdzone [S45]
15 lis 2026	**Ministerstwo Cyfryzacji** Rozwiązanie przejściowe przywraca znaczną część usług według późniejszego komunikatu [S31]
18 lis 2026	**CERT Polska** Publikuje ostrzeżenie o obsłudze tokenu w nVision [S23]
19 lis 2026	**Ministerstwo Cyfryzacji** Ogłasza pełne przywrócenie ePUAP po etapowych testach [S31]

6.4 Ostatnia aktywność: 9–22 listopada

Odtworzenie usługi publicznej ma kilka etapów. Komunikat ePUAP rozróżnia wykrycie 10 listopada, rozwiązanie przejściowe 15 listopada, usługi transakcyjne 16 listopada i pełne działanie 19 listopada. Nie wskazuje grupy ani potwierdzonej liczby skradzionych danych osobowych [S31].

Dla zależnych organizacji najważniejsza jest możliwość złożenia pisma lub wykonania procesu klienta. Sama dostępność strony głównej nie wystarcza. Zachowuj informacje o dopuszczonej alternatywie, próbach złożenia i ostatecznym przyjęciu.

Dostęp do danych płatniczych nie rozstrzyga kopiowania. Komunikat Autopay dotyczy wykrycia 11 listopada. Potwierdza dostęp, ale wyraźnie nie potwierdza kopiowania ani użycia. PRNews umieszcza publiczny komunikat w tym samym ostatnim okresie [S45][S46].

Obsługa powinna przekazywać sprawdzone instrukcje i zapewnić bezpieczne oddzwonienie. Oszust może przywołać prawdziwy komunikat. Znajomość zdarzenia nie uprawnia do żądania kodów, zmian konta ani przelewów.

Ostatni biuletyn wymaga decyzji o aktualizacji. Ostrzeżenie CERT Polska z 18 listopada opisuje token użytkownika w parametrze adresu URL nVision. Wskazuje wersje poniżej 18 jako podatne i wersję 18 jako poprawioną. Rekord NVD również wskazuje poprawkę [S23][S24].

To ujawnienie podatności, a nie liczba objętych polskich organizacji lub potwierdzonych wykorzystań. Właściciele powinni ustalić użycie produktu, odpowiednio go zaktualizować i ocenić możliwą ekspozycję tokenów na podstawie własnych logów.

Ostatni dzień jest częściowy. Datą odcięcia jest 22 listopada, ale obserwacje wykonywano w trakcie tego dnia. Raport nie obejmuje wpisów i komunikatów, które jeszcze nie istniały podczas odczytu. Listopada nie porównuje się z pełnym miesiącem jako miary intensywności zagrożeń.

Ostatnie ogłoszenia pozostają niezweryfikowane. Oferta forum z 16 listopada wycenia rzekomą skrzynkę podmiotu publicznego na 550 USD i deklaruje bieżący stan. Oferta gastronomiczna z 15 listopada deklaruje świeży eksport. To reklamy bez ustalonego dostępu, aktualności lub związku z ePUAP albo Autopay (B08, B03) [S1].

Aktualizacja przemysłowa dotyczy wcześniejszego zdarzenia. Firma przemysłowa rozszerzyła 19 listopada komunikat o ransomware wykrytym 29 października. Szyfrowanie i utrata dostępu są potwierdzone; kopiowanie i publikacja pozostają nieustalone. Najnowszym zdarzeniem jest aktualizacja informacji, a nie nowy atak [S71].

Wielonarodowa oferta zawiera oznaczenie Polski. Reklama z 12 listopada oferuje krajowe pakiety danych, w tym polski. Deklaruje około 103–255 GB na pakiet krajowy. Autentyczność, rzeczywisty skład krajowy, data pozyskania i liczba osób pozostają niezweryfikowane. Promocje z 14 i 16 listopada nie są dodatkowymi incydentami (B16) [S1].

Oznaczenie nie ustala nowego włamania do polskiej firmy ani związku z oficjalnymi komunikatami listopadowymi. Rozmiar pakietu jest deklaracją sprzedawcy, a nie pomiarem polskiej populacji danych.

Karta dowodowa B16 — 12 lis 2026

Suction19213821 | Forum | Forum | Angielski

ORYGINAŁ

Complaints, Violations and Data (~103 to ~255 GB each country package)

TŁUMACZENIE

Skargi, naruszenia i dane (~103 do ~255 GB na pakiet krajowy)

Zachowany materiał

Wielonarodowa oferta zawiera pakiet oznaczony jako Polska i deklaruje rozmiary pakietów krajowych.

Nie ustalono

Nie ustalono autentyczności, składu krajowego, rozmiaru, pochodzenia, bieżącego dostępu ani liczby osób.

6.5 Komunikacja zachowująca niepewność

Przydatny pierwszy komunikat wskazuje usługi, aktualne ograniczenia, alternatywny kanał i termin następnej aktualizacji. Powinien osobno określać, czy dostęp, kopiowanie, publikacja i użycie zostały ustalone czy nadal są badane.

Nie ogłaszaj krajowej kampanii na podstawie podobnego czasu lub narracji politycznej. Incydent dostawcy płatności i ograniczona platforma publiczna nie stają się jedną operacją bez konkretnego dowodu powiązania.

W przygotowaniu DDoS uzgodnij kontakt dostawcy, osobę uruchamiającą ochronę, pomiary i rzecznika. Ćwiczenie powinno testować aktywację oraz publiczny opis wpływu. Dowodem zakończenia jest działający proces decyzyjny i zachowane pomiary.

NAJWAŻNIEJSZE WNIOSKI

01

Publiczna deklaracja i przerwa usługi wymagają osobnej weryfikacji.

02

Listopadowe komunikaty o dostępie i odtwarzaniu zachowują własne niewyjaśnione pytania.

03

Przygotuj ochronę, alternatywne procesy i komunikację faktów przed następną deklaracją.

ROZDZIAŁ 07

Aktorzy zagrożeń i powiązania dowodowe

07

TEN ROZDZIAŁ ODPOWIADA

Które twierdzenia o aktorach są uzasadnione i czego nie należy łączyć?

56

polskich wpisów ransomware pod 21 etykietami grup

7.1 Mapa relacji: dowód przed linią połączenia 64
7.2 UNC1151/Ghostwriter: bieżąca kampania pocztowa 65
7.3 Macierz zachowań kampanii pocztowej 66
7.4 Grupy deklarujące DDoS 67
7.5 Ransomware: widoczna populacja wpisów 68
7.6 Historyczny kontekst producenta bez nowego polskiego przypadku 71
7.7 Persony i twierdzenia o wspólnym operatorze 72
7.8 Ukierunkowana kampania dokumentów według DKWOC 72
7.9 Listy celów i historyczne daty kampanii 72

ROZDZIAŁ 07

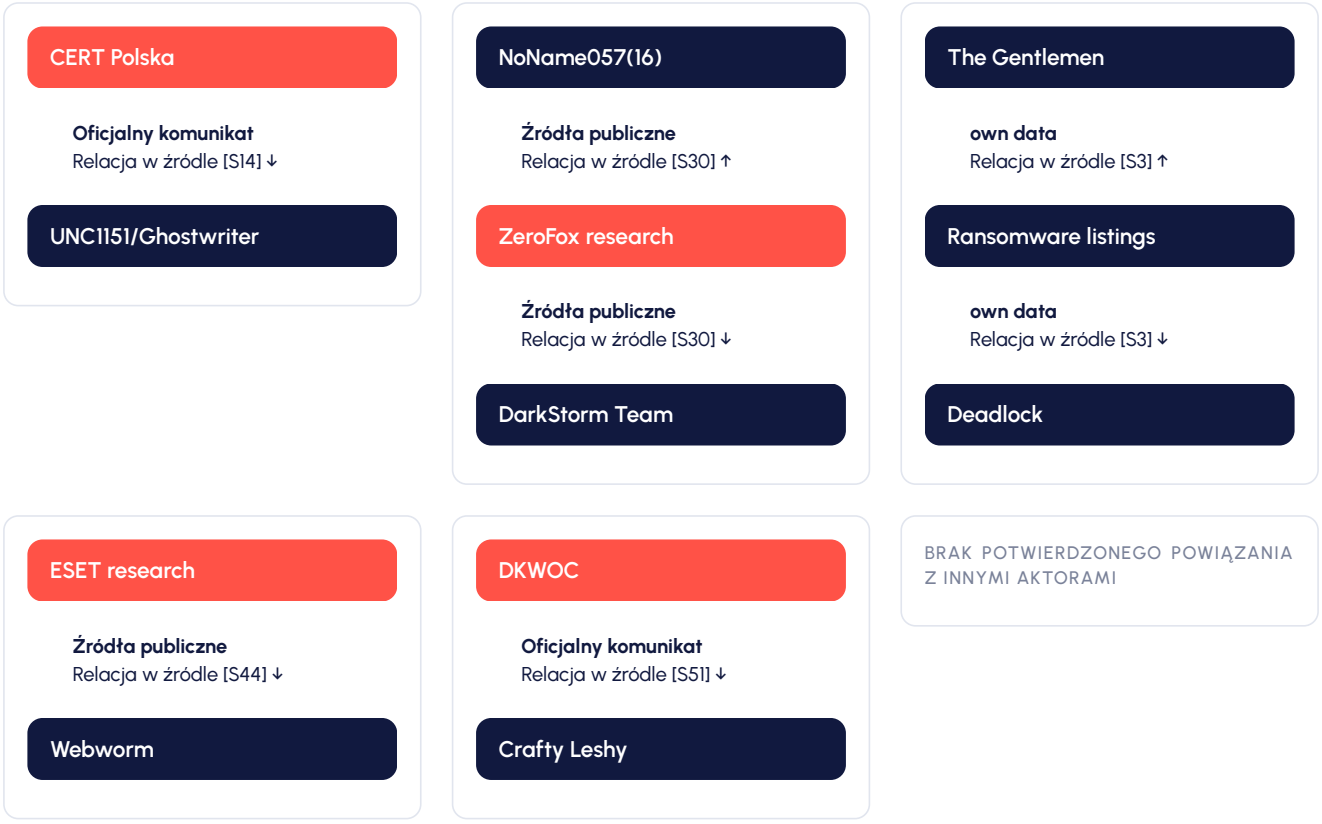
Aktorzy zagrożeń i powiązania dowodowe

W SKRÓCIE

CERT Polska przypisuje bieżącą kampanię phishingową UNC1151/Ghostwriter. Publiczne badania opisują deklaracje DDoS i historyczny kontekst szpiegostwa. Ransompedia zawiera 56 polskich wpisów, z największą liczbą pod etykietą The Gentlemen. Źródła opisują różne populacje i nie ustalają jednej sieci operacyjnej. Dobieraj zabezpieczenia do zachowania i zachowuj granice przypisania podane przez źródło.

7.1 Mapa relacji: dowód przed linią połączenia

Mapa odróżnia oficjalne przypisanie kampanii, publiczne badania i obserwacje wpisów. Nie łączy aktorów tylko dlatego, że wspominają Polskę, używają tego samego języka lub pojawiają się w tym samym miesiącu.



Relacja	Dowód	Co uzasadnia	Czego nie uzasadnia
CERT Polska i kampania UNC1151/Ghostwriter	Oficjalne badanie [S14]	Identyfikację kampanii i zachowania według źródła	Liczby ofiar lub niezależnego przypisania państwu
ZeroFox i deklaracje NoName057(16) oraz DarkStorm Team	Publiczne badanie [S30]	Obserwację styczniowych ogłoszeń	Zweryfikowanego wpływu lub związku z listopadowymi incydentami
Ransompedia i etykieta The Gentlemen	Obserwacja wpisów [S3]	Dziewiętnaście wpisów przypisanych Polsce w zbiorze	Szyfrowania w każdym przypadku lub wspólnego operatora
ESET i Webworm	Badanie producenta [S44]	Identyfikację i ocenę powiązania z Chinami według ESET dla kampanii głównie z 2025	Nowego potwierdzonego włamania w Polsce w 2026

Żaden z tych związków nie dostarcza konkretnego dowodu wspólnej organizacji dla phishingu, deklaracji DDoS i wymuszeń. Model łączący sprzedawcę dostępu, posiadacza danych i oszusta byłby modelem analitycznym, a nie ustalonym łańcuchem przestępczym.

7.2 UNC1151/Ghostwriter: bieżąca kampania pocztowa

Czerwcowa relacja CERT Polska wskazuje rozpoczęcie ataków na Gmail w marcu 2026. Wiadomości naśladowały ostrzeżenia, stosowały presję po polsku i wyłudzały hasła oraz kody drugiego składnika. Wskazane role obejmują administrację, badaczy, dziennikarzy i ich bliskich [S14].

Źródło opisuje dedykowane strony phishingowe i nadużywane usługi internetowe. Wymienia też poszukiwane po dostępie kontakty, dokumenty i powiązane konta. Uzasadnia to ochronę uprawnień logowania i obserwację poczty.

Nie dowodzi, że każda wiadomość dotarła do zamierzonej osoby lub każda próba logowania się powiodła. Raport nie przypisuje kampanii państwu samodzielnie. Nie uznaje też publicznej funkcji danej osoby za dowód jej celowego wytypowania.

UNC1151/Ghostwriter

Kampania phishingu pocztowego | Identyfikacja CERT Polska; brak samodzielnego przypisania państwu

W POLSCE, 2026

Marzec 2026
Początek kampanii Gmail według CERT

12 czerwca 2026
Publikacja oficjalnej analizy

DEKLAROWANE CELE

Role i osoby powiązane wskazane przez CERT Polska

W ŹRÓDŁACH PUBLICZNYCH

[S14] Zakres opisany w źródle

NASZA OCENA

Weryfikuj logowania i pocztę. Opisana ścieżka obejmuje wyłudzanie kodów drugiego składnika.

POZIOM PEWNOŚCI
Wysoka dla relacji urzędowej; wyniki wymagają dowodów konta

7.3 Macierz zachowań kampanii pocztowej

To analityczne przyporządkowanie zachowań opisanych przez CERT Polska do MITRE ATT&CK, wykonane przez Odin. Nie oznacza, że CERT podał te identyfikatory. Definicje technik odczytano w MITRE [S47][S48][S49][S50].

ANALITYCZNE PRZYPISANIE ZACHOWAŃ KAMPANII POCZTOWEJ DO TECHNIK MITRE

Dostarczenie	Dane dostępowe	Użycie konta	Zbieranie
T1566.002 Odnośnik phishingowy	T1111 Przechwycenie drugiego składnika	T1078 Poprawne dane konta	T1114.002 Zdalne zbieranie poczty

Analityczne przyporządkowanie Odin zachowań opisanych przez CERT Polska do definicji MITRE. Nie jest mapowaniem źródła ani przetestowaną detekcją. [S14]

Zachowanie	ATT&CK	Zakres wsparty źródłem	Pytanie obrońcy
Odnośnik w wiadomości udającej ostrzeżenie	T1566.002	Opisana droga dostarczenia [S14][S47]	Czy odbiorca może zgłosić przynętę bez otwierania odnośnika?
Przechwycenie kodu drugiego składnika	T1111	Opisane zbieranie kodu i próba logowania [S14][S48]	Czy ważne logowania są odporne na przekazywanie danych dostępowych?
Użycie uzyskanych danych logowania	T1078	Opisana próba dostępu do prawdziwego konta [S14] [S49]	Czy podejrzane użycie można powiązać z sesją?
Przeszukiwanie dostępnej skrzynki	T1114.002	Opisany cel zbierania; brak krajowej liczby sukcesów [S14][S50]	Czy logi dostępu i eksportu poczty docierają do reagowania?

Macierz jest wskazówką do weryfikacji, a nie regułą wykrywania ani sprawdzonym pokryciem. Trzeba przełożyć ją na telemetrię organizacji i przetestować przed uznaniem za działającą detekcję.

7.4 Grupy deklarujące DDoS

Opisy NoName057(16) i DarkStorm Team pochodzą z badania ZeroFox. Ocena orientacji politycznej pozostaje przypisana źródłu. Styczniowe obserwacje uzasadniają gotowość usługową, a nie przypisanie każdej polskiej awarii [S30].

NoName057(16)

Grupa deklarująca DDoS | Według ZeroFox prorosyjska; nie ustalono kierowania państwowego

W POLSCE, 2026

12 stycznia 2026
Deklaracje obserwowane przez ZeroFox

13 września 2026
Zachowana deklaracja dotycząca Polski (B07)

DEKLAROWANE CELE

Ogólne usługi publiczne i komercyjne; identyfikatory ukryte

ICH SŁOWAMI

"Poland [...]" B07

W ŹRÓDŁACH PUBLICZNYCH

[S1] Zakres opisany w źródle

[S30] Zakres opisany w źródle

NASZA OCENA

Ogłoszenie i odnośniki dostępności nie ustalają czasu, wpływu ani odpowiedzialności za listopad.

POZIOM PEWNOŚCI

Wysoka dla zachowania wpisu; wpływ niezweryfikowany

DarkStorm Team

Grupa deklarująca DDoS | Brak samodzielnego przypisania państwu

W POLSCE, 2026

12 stycznia 2026

Deklaracje dotyczące Polski w publicznym badaniu

DEKLAROWANE CELE

Organizacje opisane w cytowanym badaniu

W ŹRÓDŁACH PUBLICZNYCH

[S30] Zakres opisany w źródle

NASZA OCENA

Korzystaj z pomiarów operatora przed przyjęciem twierdzeń o wpływie. Nie ustalono związku z listopadem.

POZIOM PEWNOŚCI

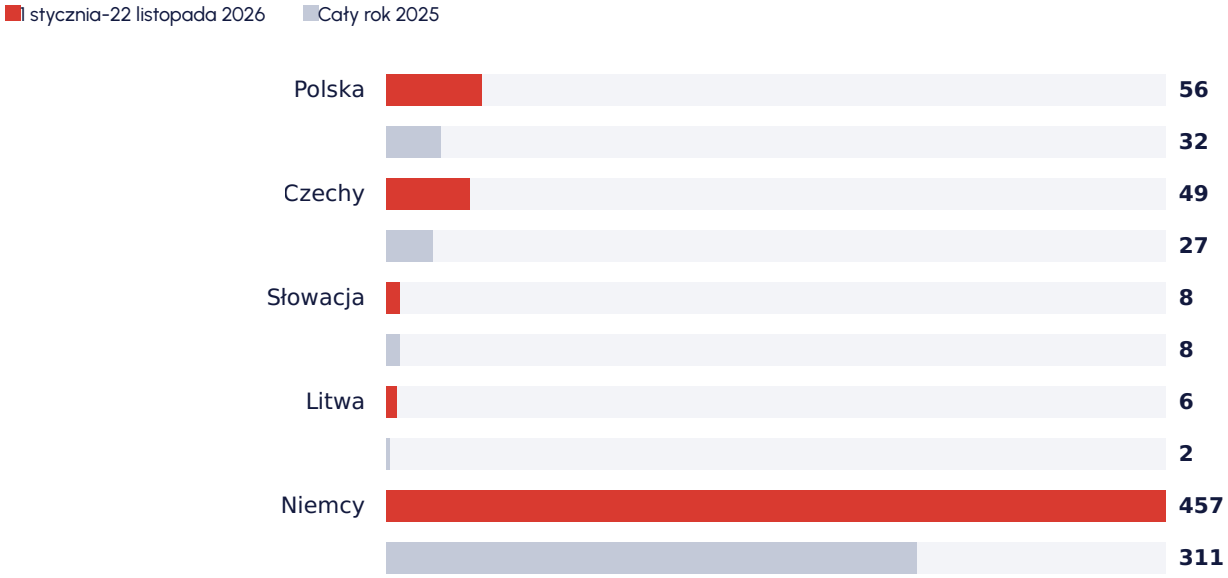
W zakresie podanym przez ZeroFox

Organizacja nie powinna przyjmować języka grupy jako własnego wyjaśnienia publicznego. Potwierdź rzeczywisty proces, stan ochrony i etap przywracania. Pomiar dostawcy jest silniejszym dowodem wpływu niż zrzut ekranu grupy.

7.5 Ransomware: widoczna populacja wpisów

Ransompedia zawiera 56 wpisów oznaczonych jako Polska w okresie 2026 oraz 32 za cały 2025. Okresy są różne. Nie jest to roczne tempo wzrostu, liczba potwierdzonych ofiar ani miara prawdopodobieństwa ataku w kraju [S3].

Regionalne liczby wpisów opisują widoczność, a nie ryzyko kraju



Źródło: zbiór wpisów Brandefense Ransompedia. Rok 2026: 1 stycznia–22 listopada; 2025: cały rok. Różne okresy; nie jest to krajowy ranking ryzyka [S3].

Kraje do porównania wybrano jako przykłady wyłącznie w celu przedstawienia kontekstu; ich wybór nie oznacza rankingu ani oceny politycznej.

Kraj	Okres 2026	Cały 2025	Interpretacja
Polska	56	32	Część roku porównana z pełnym rokiem
Czechy	49	27	Sąsiednia gospodarka przemysłowa i usługowa
Słowacja	8	8	Mniejsza sąsiednia gospodarka produkcyjna i transportowa
Litwa	6	2	Bliski bałtycki partner usługowy i logistyczny
Niemcy	457	311	Większa sąsiednia gospodarka; bez korekty wielkości

Czterech partnerów wybrano ze względu na geografię i zależności usługowe. Nie tworzą grupy politycznej. Etykiety krajowe pochodzą ze źródła i mogą wymagać weryfikacji organizacji; raport nie tworzy na ich podstawie rankingu bezpieczeństwa państw.

Największe polskie etykiety to The Gentlemen z 19 wpisami, Deadlock z pięcioma, Coinbasecartel i Nova po cztery oraz Qilin z trzema. Szesnaście dalszych etykiet odpowiada za 21 wpisów. Największa etykieta obejmuje więc 33,9% z 56 obserwacji.

The Gentlemen

Etykieta wpisów ransomware | Twierdzenia o wymuszeniach; brak przypisania państwu

W POLSCE, 2026

Okres 2026

19 wpisów oznaczonych jako Polska

DEKLAROWANE CELE

Kilka kategorii branżowych; bez publicznej listy ofiar

W ŹRÓDŁACH PUBLICZNYCH

[S3] Zakres opisany w źródle

NASZA OCENA

Największa etykieta w zbiorze. Nie dowodzi wspólnych operatorów ani szyfrowania każdego przypadku.

POZIOM PEWNOŚCI

Wysoka dla liczb źródła, nie wyników

Deadlock

Etykieta wpisów ransomware | Twierdzenia o wymuszeniach; brak przypisania państwu

W POLSCE, 2026

Okres 2026

Pięć wpisów oznaczonych jako Polska

DEKLAROWANE CELE

Kategorie branżowe przypisane przez źródło

W ŹRÓDŁACH PUBLICZNYCH

[S3] Zakres opisany w źródle

NASZA OCENA

Przygotuj odtwarzanie niezależne od nazwy grupy i sprawdzaj pasujący zarzut.

POZIOM PEWNOŚCI

Wysoka dla liczb źródła

Miesięczne liczby polskie sumują się do 56. Lipiec zawiera dziesięć wpisów, kwiecień osiem, a styczeń siedem. Listopad ma trzy w chwili obserwacji i pozostaje częściowy. Daty dotyczą publikacji lub daty zastępczej źródła, nie początku włamania.

Połączone kategorie obejmują 17 wpisów technologicznych, 13 przemysłowych, osiem edukacyjnych, siedem konsultingowych i jedenaście z innych sektorów. To wpisy, a nie niezależnie policzone organizacje. Nie połączono ich z próbą wybranych domen.

7.6 Historyczny kontekst producenta bez nowego polskiego przypadku

Badanie ESET z maja 2026 opisuje aktywność Webworm z 2025 i wskazuje cele rządowe w Polsce wśród kilku krajów europejskich. ESET określa grupę jako powiązaną z Chinami oraz opisuje kanały sterowania w chmurze i narzędzia proxy [S44].

Źródło opisuje też aktywność do stycznia 2026 dotyczącą podmiotu hiszpańskiego. Nie ustala to styczniowego włamania w Polsce. Polskie cele pozostają historycznym kontekstem ujawnionym w 2026.

Webworm

Historyczny kontekst szpiegostwa | Według ESET powiązana z Chinami

W POLSCE, 2026

Aktywność 2025

Polskie cele rządowe opisane w maju 2026

DEKLAROWANE CELE

Organizacje rządowe w kilku krajach

W ŹRÓDŁACH PUBLICZNYCH

[S44] Zakres opisany w źródle

NASZA OCENA

Źródło dotyczy głównie 2025. Aktywność w innym kraju nie dowodzi nowego polskiego włamania w styczniu 2026.

POZIOM PEWNOŚCI

Według przypisania i dat ESET

Obrońcy powinni sprawdzić nietypowe korzystanie przez serwery z komunikatorów, udostępniania plików i usług proxy. Przypisanie grupy przez producenta nie zastępuje lokalnej weryfikacji legalnych aplikacji i administracji.

7.7 Persony i twierdzenia o wspólnym operatorze

Alias jest etykietą ogłoszenia lub wypowiedzi. Zgodne nazwy nie dowodzą tożsamości prawnej, a różne nazwy nie dowodzą różnych ludzi. Twierdzenia o incydencie medycznym i biznesowym można łączyć tylko na poziomie uzasadnionym dowodami.

Komunikat FELG i relacja AHA pokazują znaczenie ostrożności: osoba deklarowała przynależność, a publiczne badanie opisywało innego aktora. Raport zachowuje obie relacje i nie ustala wspólnej własności na podstawie marki [S8][S9].

Karty zachowują oryginalny język tylko wtedy, gdy pomaga w obronie. Kontakty, identyfikatory celów i retorykę polityczną usunięto. Wspólne ogłoszenie uzasadnia relację reklamową, a nie tożsamość pliku, drogi dostępu lub zakończonej transakcji.

7.8 Ukierunkowana kampania dokumentów według DKWOC

DKWOC opisuje identyfikację artefaktów kampanii 30 stycznia 2026, obejmującej instytucje krajowe i zagraniczne. Śledzi ją jako Crafty Leshy i przytacza przyporządkowanie CERT-UA do UAC-0001/APT28. Oba oznaczenia pozostają ocenami konkretnych źródeł [S51].

Oficjalna relacja opisuje wiadomości związane z działalnością instytucji, wysyłane z wcześniej dostępnych skrzynek, oraz złośliwe dokumenty Office. Nie podaje liczby polskich ofiar. Pierwotna strona nie ujawnia daty publikacji, dlatego raport korzysta z wyraźnie wskazanej daty obserwacji.

Dla CVE-2026-21509 NVD wymienia rodziny produktów Office. Biuletyn Microsoft rozróżnia ochronę starszych wydań i edycji chronionych po stronie usługi. Zweryfikowane wersje podano w dodatku A; otwarcie biuletynu nie dowodzi zastosowania poprawki [S52][S53].

7.9 Listy celów i historyczne daty kampanii

Analiza Manic ThreatFabric z 20 sierpnia wprost uwzględnia Polskę w celach aplikacji bankowych i państwowej tożsamości. Daty infrastruktury sięgają lutego, a zachowane komponenty pojawiają się później. Lista ustala zamierzony zakres aplikacji, bez liczby polskich infekcji lub dowodu dostępu do infrastruktury banku [S86].

Analiza RemControl Group-IB z 23 września obejmuje Polskę w celach nakładek finansowych. Szczegółowy przykład dostarczenia i oznaczenia kampanii dotyczą innych obszarów. Obsługiwana polska nakładka nie ustala dotarcia obserwowanej dystrybucji do polskich użytkowników; nie podano miejscowej liczby ofiar [S87].

Lutowa publikacja Shadow Campaigns Unit 42 umieszcza polskie cele rządowe w 2025. Osobna aktywność styczniowa dotyczy innego państwa. To kontekst historyczny, a nie nowo ustalony polski incydent 2026. Oznaczenia badawcze i ocena powiązania z państwem pozostają przypisaniem Unit 42, bez niezależnej atrybucji autorów [S88].

NAJWAŻNIEJSZE WNIOSKI

01

Przypisuj każdy opis aktora i powiązanie państwowe do źródła.

02

Dobieraj zabezpieczenia do zachowań i lokalnej weryfikacji, a nie nazwy grupy.

03

Oddziel etykiety wpisów, deklaracje person i potwierdzone incydenty.

ROZDZIAŁ 08

Ekonomia oszustw

08

TEN ROZDZIAŁ ODPOWIADA

Jak dane tożsamości mogą stać się fałszywą dyspozycją lub obciążeniem?

3

odrębne pytania: tożsamość, uprawnienie i transakcja

8.1 Informacja i uprawnienie to różne zasoby 75
8.2 Materiały kartowe: wąski zakres 75
8.3 Handel kontami i dokumenty tożsamości 75
8.4 Oszustwo mobilne wykracza poza płatność kartą 76
8.5 Poczta biznesowa i zmiany płatnicze 76
8.6 Cena ofertowa nie oznacza wartości rynku 76
8.7 Praktyczne przekazanie sprawy 77
8.8 Oficjalne obserwacje kampanii w ciągu roku 77
8.9 Kontekst kampanii i działań organów ścigania 78

ROZDZIAŁ 08

Ekonomia oszustw

W SKRÓCIE

Wiarygodna wiadomość może zawierać prawdziwe dane osobowe lub biznesowe bez rzeczywistego uprawnienia. Ujawnienia i badania złośliwych aplikacji pokazują potrzebę niezależnej kontroli odzyskiwania kont, zmian odbiorców i rozmów ze wsparciem. Ogłoszenia podziemia opisują podaż i popyt, a nie wykonane transakcje lub krajowe straty. Zachowaj wąski zakres materiałów kartowych i testuj decyzję biznesową, którą oszust chce zmienić.

8.1 Informacja i uprawnienie to różne zasoby

Imię, adres, wzmianka o zdrowiu lub prawdziwa faktura mogą uwiarygodnić wiadomość. Nie potwierdzają, że nadawcą jest bank, placówka lub prawidłowy dostawca. Ujawnienia MyDr, uczelni i systemu księgowego nadają temu rozróżnieniu praktyczne znaczenie [S5][S10][S41].

Sam komunikat o incydencie może stać się pretekstem. Rozmówca może przywołać rzeczywiste zdarzenie i proponować ochronę konta, weryfikację pacjenta lub przeniesienie pieniędzy. Personel powinien rozpoznawać zdarzenie bez nadawania rozmówcy uprawnień.

Najpierw ustal, czy kontakt rozpoczęto zaufaną drogą. Następnie sprawdź uprawnienie do żądanej czynności. Na końcu potwierdź transakcję lub ujawnienie danych. Zastąpienie tych pytań testem znajomości danych osobowych tworzy słaby punkt decyzji.

8.2 Materiały kartowe: wąski zakres

ZAKRES LICZB NA KARTACH

Liczby obejmują wyłącznie karty płatnicze widoczne jawnie we wpisach podziemia zgromadzonych do raportu. Brandefense wykrywa skradzione karty także wieloma innymi metodami poza tym raportem. Wyniki nie mierzą kradzieży kart ani strat z oszustw.

Zachowane wpisy zawierają 455 odrębnych kart związanych z Polską w 413 wpisach. Wśród nich 76 powiązano z wydawcami, a 379 wyłącznie z krajem. Grupy są rozłączne. Nie opublikowano tabeli wydawców; nie ustalono ważności kont, udanych płatności ani strat [S4].

8.3 Handel kontami i dokumenty tożsamości

Ogłoszenie konta lub pakietu tożsamości dowodzi złożenia oferty. Nie ustala aktywności konta, autentyczności dokumentów, kontroli sprzedawcy ani wykonania transakcji. Karty zachowują te ograniczenia [S1].

Dla obrońcy istotna bywa rejestracja lub odzyskiwanie konta. Usługa powinna określać weryfikację tożsamości, zatwierdzanie nowego urządzenia i uprawnienie do obejścia nieudanego sprawdzenia. Skradziony obraz dokumentu nie powinien sam wystarczać do nadania dostępu.

Odzyskiwanie przez SIM i telefon wymaga wspólnej odpowiedzialności. Obsługa, tożsamość i operator mogą posiadać różne fragmenty dowodów. Syntetyczne ćwiczenie powinno wykazać zatrzymanie nietypowego odzyskiwania bez trwałego wykluczenia prawidłowego klienta.

Zachowana reklama rekrutacji do oszustw najmu opisuje proces ukierunkowany na Polskę, obejmujący opłaty z góry za dokumenty, ubezpieczenie i rezerwację. Potwierdza reklamę rekrutacji i deklarowany proces, bez ustalonej liczby ofiar lub strat. Komunikacja mieszkaniowa i studencka powinna jasno wskazywać niezależną weryfikację [S1].

8.4 Oszustwo mobilne wykracza poza płatność kartą

Wrześniowa analiza CERT Polska powiązała 852 z 1 235 obserwowanych reklam z 17 aplikacjami przez wspólny kod lub infrastrukturę. Opisuje drogę do wiadomości premium i płatności operatorskich. Liczby dotyczą reklam i aplikacji, a nie ofiar lub obciążeń [S15].

Wymaga to innej ochrony klienta niż wymiana karty. Abonent może potrzebować sprawdzenia płatności operatorskich, usunięcia aplikacji i odzyskania konta. Właściwa reakcja zależy od rzeczywistych dowodów aplikacji i transakcji.

Analiza FvncBot pokazuje inną ścieżkę: wiarygodny motyw finansowy, a następnie dodatkową instalację i uprawnienia dostępności. Zaobserwowany wizerunek nie dowodzi incydentu wewnątrz naśladowanej instytucji [S16].

8.5 Poczta biznesowa i zmiany płatnicze

Incydenty dostawców i księgowości mogą ujawnić szczegóły uwiarygodniające fałszywą dyspozycję. Kluczowe jest niezależne potwierdzenie uprawnienia do zmiany przy użyciu kontaktu znanego wcześniej. Druga osoba zatwierdzająca tę samą niesprawdzoną wiadomość może powtórzyć błąd.

Przetestuj syntetyczne żądanie zmiany rachunku dostawcy, pilne polecenie kierownictwa i rzekomy telefon wsparcia. Oczekiwany wynik to bezpieczne wstrzymanie, niezależne potwierdzenie i jasny zapis zatwierdzenia.

Przy poczcie zachowaj logowania, sesje, reguły i odpowiednie wiadomości. Przy urządzeniu końcowym połącz izolację z naprawą kont i sesji. Raport nie zakłada, że każda fałszywa dyspozycja zaczęła się od malware lub incydentu pocztowego.

8.6 Cena ofertowa nie oznacza wartości rynku

Wybrane oferty podają ceny dla różnych jednostek [S1].

Karta	Reklamowany przedmiot	Cena	Granica
B01	Deklarowany dostęp do serwera	200 USD	Dostęp niezweryfikowany; brak wykonanej transakcji
B08	Rzekoma usługa skrzynki podmiotu publicznego	550 USD	Stan i kontrola skrzynki niezweryfikowane
B10	Deklarowany plik serwisu ogłoszeń	1 980 USD	Wielkość, pochodzenie i sprzedaż niezweryfikowane

Cena może dotyczyć dostępu, pliku, subskrypcji lub usługi dla kupującego. Waluta, wielkość, aktualność i wyłączność mogą być deklaracjami. Nie należy łączyć cen różnych jednostek ani traktować ich jako zrealizowanych przychodów.

Dotyczy to także popytu. Wiele powtórzeń może pochodzić od jednego wytrwałego reklamodawcy. Zapytanie kupującego dowodzi wyrażonego zainteresowania, bez potwierdzenia zakupu lub nowego incydentu.

8.7 Praktyczne przekazanie sprawy

Sygnał	Pierwszy właściciel	Weryfikacja	Dowód zamknięcia
Bieżąca oferta konta lub dostępu	Tożsamość i SOC	Status konta, sesje i wcześniejsze działania	Uzasadniona decyzja i proporcjonalna reakcja
Zmieniony odbiorca płatności	Finanse	Potwierdzenie ze znaną wcześniej osobą	Niezależne zatwierdzenie lub odrzucenie zmiany
Podejrzane obciążenie mobilne	Przeciwdziałanie oszustwom i operator	Droga rozliczenia i kontekst aplikacji	Rozstrzygnięcie sprawy klienta i właściwa naprawa dostępu
Rozmowa powołująca się na incydent	Obsługa klienta	Zakończenie i kontakt ustaloną drogą	Bezpieczny ponowny kontakt bez udostępniania kodu
Zarzut dotyczący pacjenta lub studenta	Prywatność i właściciel usługi	Odpowiednie rekordy i zakres administratora	Ukierunkowana porada i zapisana decyzja o zawiadomieniu

8.8 Oficjalne obserwacje kampanii w ciągu roku

Miesięczne podsumowania CERT Polska dodają kontekst kampanii poza incydentami nazwanych organizacji. To powtarzające się wzorce ostrzeżeń, a nie dziesięć odrębnych incydentów ofiar.

Miesiąc	Opisany wzorzec	Działanie obrońcy
Styczeń	Żądania podszywające się pod policję [S61]	Sprawdź instytucję znanym kanałem

Miesiąc	Opisany wzorzec	Działanie obrońcy
Luty	Phishing opłat za dostawę [S62]	Otwórz zaufaną usługę samodzielnie
Marzec	Żądania dokumentów pod pozorem organu [S63]	Nie wysyłaj dokumentu niezweryfikowanemu kontaktowi
Kwiecień	Wyłudzanie hasła i kodu przy aktualizacji SIM [S64]	Sprawdź żądanie u operatora
Maj	Opłaty za studia z przejętych skrzynek uczelnianych [S65]	Sprawdź dyspozycję poza wiadomością
Czerwiec	Złośliwe załączniki potwierdzeń płatności [S66]	Sprawdź nadawcę i zastosuj proces bezpieczeństwa
Lipiec	SMS phishing opłat parkingowych [S67]	Użyj samodzielnie otwartej usługi płatniczej
Sierpień	Oszustwo QR łączenia urządzenia komunikatora [S68]	Sprawdź urządzenia i odrzuć niezweryfikowane dodanie
Wrzesień	Przynęty urzędowe z fałszywym logowaniem bankowym [S69]	Sprawdź usługę przed podaniem danych
Październik	Załączniki podatkowe ze zdalnym malware [S70]	Zgłoś podejrzany załącznik bez otwierania

8.9 Kontekst kampanii i działań organów ścigania

Analiza cifrat CERT Polska z 3 kwietnia opisuje łańcuch zdalnego dostępu na Androidzie dostarczany jako rzekoma aktualizacja aplikacji hotelarskiej. Źródło nie mogło wiarygodnie przypisać malware do istniejącej rodziny. Analiza nie podaje liczby objętych polskich organizacji [S82].

Komunikat CBZC z 31 marca opisuje dochodzenie dotyczące phishingu bankowego i kurierskiego. Data operacji nie ustala początku kampanii ani nie umieszcza wszystkich strat w 2026. Lipcowe dochodzenie płatnych usług DDoS również nie ustala liczby ofiar lub ataków; podejrzani nie są przedstawiani jako skazani [S84][S85].

Komunikat CBZC z 13 listopada opisuje prowadzoną w Polsce operację dotyczącą oszustw fakturowych. Wymienione państwa ofiar były poza Polską. To kontekst sprawdzania dyspozycji płatniczych, a nie liczba polskich organizacji ofiar ani dowód prawomocnego skazania [S83].

NAJWAŻNIEJSZE WNIOSKI

01

Prawdziwe dane nie nadają uprawnienia do zmiany konta lub płatności.

02

Płatności operatorskie i złośliwe aplikacje wymagają szerszej reakcji niż kontrola karty.

03

Traktuj ogłoszenia i ceny jako deklaracje z wyraźną jednostką transakcji.

ROZDZIAŁ 09

Bankowość i finanse

09

TEN ROZDZIAŁ ODPOWIADA

Jakie zabezpieczenia tożsamości i oszustw wynikają z obserwacji wybranych domen finansowych?

10 z 30

wybranych domen finansowych z ofertą danych logowania

9.1 Populacja i ograniczenia 80
9.2 Pracownicy, klienci i współdzielone tożsamości 81
9.3 Informacje płatnicze mogą być prawidłowe, a dyspozycja fałszywa 82
9.4 Aplikacje mobilne zmieniają granicę oszustwa 82
9.5 Ostatni incydent dostawcy płatności 82
9.6 Wspólna odpowiedzialność za odporność finansową 83

ROZDZIAŁ 09

Bankowość i finanse

W SKRÓCIE

Dane logowania powiązane z 10 z 30 wybranych domen finansowych były oferowane w momencie sprawdzenia. Portfel obejmuje co najmniej 80 757 powiązań urządzeń, w tym 304 pracowniczych. Dopasowany podzbiór wydawców ma odrębny zakres. Komunikat Autopay potwierdza dostęp, pozostawiając kopiowanie niewyjaśnione. Sprawdzaj bieżące konta i dyspozycje płatności, równolegle badając dostęp pracowników i chroniąc klientów.

9.1 Populacja i ograniczenia

Portfel finansowy obejmuje 30 domen kandydackich banków, płatności i infrastruktury rynku. Nie stanowi listy wszystkich licencjonowanych banków lub wydawców kart. Powiązania ekspozycji nie mierzą nadużyć kont w całej Polsce [S2].

Miara	Wynik	Granica
Domeny finansowe	30	Wybrani kandydaci, nie wszystkie regulowane podmioty
Domeny z bieżącą ofertą	10 / 30	Oferta danych logowania, nie potwierdzony dostęp do infrastruktury
Powiązania urządzeń	≥80 757	Obejmuje pracowników; właściciel pozostałych nieustalony
Powiązania urządzeń pracowników	304	Zawarte w powyższej sumie
Historyczne rekordy logowania	54 584	Nie są odrębnymi osobami lub aktywnymi kontami
DMARC kwarantanna lub odrzucenie	24 / 30	Żądanie polityki, nie dowód pełnego egzekwowania
Monitorowanie DMARC	6 / 30	Przed zmianą sprawdź prawidłowych nadawców
Udana walidacja TLS	30 / 30	Obserwowane połączenie, nie każdy punkt końcowy
Zaobserwowany HSTS	24 / 25	Tylko odpowiadające strony

Dopasowanie wydawców obejmuje 21 domen kandydackich z ustalonej listy banków. Szerszy portfel obejmuje też pozabankowe usługi finansowe i infrastrukturę rynku. Podzbiór nie jest zweryfikowanym krajowym spisem wydawców [S2][S4].

Dopasowany podzbiór	Wynik
Dopasowane kandydackie domeny banków	21
Dopasowane domeny z bieżącą ofertą	8
Pozostałe powiązania urządzeń	49 440
Powiązania urządzeń pracowników	272
Udział trzech największych w pozostałych urządzeniach	62,2%

Procent koncentracji dotyczy powiązań urządzeń w dopasowanym podzbiorze, a nie kradzieży kart, strat lub potwierdzonych włamań do banków. Pozostałe urządzenia są poza klasyfikacją pracowniczą; własność klientów jest możliwa, lecz nieustalona. Historyczne dane logowania i bieżące oferty zachowują osobne granice poprawności kont.

ZAKRES LICZB NA KARTACH

Dane kart obejmują wyłącznie karty widoczne jawnym tekstem w zebranych wpisach. Brandefense wykrywa skradzione karty wieloma innymi metodami poza raportem. Wartości nie mierzą kradzieży, poprawności kart lub strat oszustw.

Zachowane wpisy zawierają 455 odrębnych kart powiązanych z Polską w 413 wpisach: 76 powiązanych z wydawcami i 379 wyłącznie z krajem, w rozłącznych grupach [S4]. Obserwacji kart nie dodaje się do urządzeń lub danych logowania. Nie publikuje się rankingu banków ani przypisanych im wartości kart.

9.2 Pracownicy, klienci i współdzielone tożsamości

Urządzenie powiązane z domeną finansową może należeć do klienta, pracownika, kontrahenta lub innego użytkownika. Rekord danych logowania może dotyczyć wycofanego konta lub ponownie użytego adresu. Te różnice powinny wyznaczać pierwszą weryfikację.

Analiza dostępu pracownika sprawdza aktywność konta, uprawnienia, sesje i zarządzanie urządzeniem. Analiza oszustwa klienta ocenia prawdziwość transakcji, odzyskiwania konta lub nowego odbiorcy. Żadna ścieżka nie powinna czekać na nieuzasadnione założenie o właścicielu urządzenia.

Historyczne dane tożsamości mogą pomagać oszustowi po zmianie haseł. Obsługa powinna więc odróżniać znajomość danych od uprawnienia do działania. Wrażliwe zmiany potwierdzaj wcześniej ustalonym kanałem i jasno wyjaśniaj klientowi przyczynę.

9.3 Informacje płatnicze mogą być prawidłowe, a dyspozycja fałszywa

Potwierdzony zakres Fakturowni obejmuje kontekst biznesowy mogący uwiarygodnić instrukcję. Firma osobno podaje brak przechowywania haseł bankowych i danych kart. Incydent faktur wymaga innej reakcji niż incydent danych logowania do banku [S10].

Przy zmianie odbiorcy finanse powinny sprawdzić dyspozycję ze znaną osobą i zapisać wynik. Bezpieczeństwo może badać odpowiednią skrzynkę, konto i dostawcę. Prawdziwy numer faktury nie powinien omijać niezależnego zatwierdzenia.

Ta sama zasada dotyczy pilnych żądań powołujących się na publiczny incydent. Oszust może żądać przeniesienia pieniędzy na chronione konto albo kodu bezpieczeństwa do dochodzenia. Pracownik powinien zakończyć kontakt i skorzystać z ustalonej ścieżki.

9.4 Aplikacje mobilne zmieniają granicę oszustwa

Analiza FvncBot opublikowana przez CERT Polska opisuje aplikację z motywem bankowym prowadzącą do kolejnych modułów i uprawnień dostępności. W momencie analizy nie ustalono sposobu dystrybucji. Wizerunek banku jest przynętą, a nie dowodem dostępu do jego systemów [S16].

Wrześniowa analiza toll fraud opisuje odmienną ścieżkę: złośliwe aplikacje i płatności operatorskie. Obciążenie może więc nastąpić poza zwykłą płatnością kartą. Banki, operatorzy i obsługa potrzebują wspólnej eskalacji, bez założenia, że obie kampanie prowadzi ten sam sprawca [S15].

Na urządzeniach zarządzanych oceniaj instalowanie aplikacji i zmiany wrażliwych uprawnień. Klientom przekazuj konkretną zasadę: kontakt z bankiem nie powinien wymagać niezweryfikowanego komponentu bezpieczeństwa. Scenariusz obsługi powinien zapewniać bezpieczny ponowny kontakt z instytucją.

9.5 Ostatni incydent dostawcy płatności

Listopadowy komunikat Autopay wymaga ukierunkowanej weryfikacji. Potwierdza nieautoryzowany dostęp do infrastruktury i informacji o płatnościach, lecz nie potwierdza kopiowania ani użycia. Zaleca kontrolę transakcji i zgłaszanie nieautoryzowanych operacji bankowi [S45].

Nie wymieniaj automatycznie wszystkich kart i nie zakładaj objęcia każdego klienta. Korzystaj ze sprawdzonych instrukcji dostawcy i banku, dowodów dla konta oraz właściwego procesu reagowania. Działanie zakłócające usługę powinno mieć właściciela dowodów i zapisane uzasadnienie.

9.6 Wspólna odpowiedzialność za odporność finansową

Zespół	Decyzja	Dowód wykonania
Tożsamość i SOC	Czy zewnętrzny sygnał dotyczy aktywnego konta lub podejrzanej sesji?	Udokumentowana weryfikacja i proporcjonalna reakcja
Przeciwdziałanie oszustwom i obsługa	Czy klient lub dyspozycja są prawdziwi?	Niezależne potwierdzenie i bezpieczny kontakt
Finanse i zakupy	Czy zmiana rachunku dostawcy jest uprawniona?	Potwierdzenie ze znaną osobą i zatwierdzenie płatności
Operacje i zgodność	Czy incydent podlega właściwemu raportowaniu finansowemu?	Fakty o usłudze i zatwierdzona decyzja [S28]
Infrastruktura i właściciel biznesowy	Czy proces płatniczy można odtworzyć niezależnie?	Sprawdzona transakcja i akceptacja biznesowa

NAJWAŻNIEJSZE WNIOSKI

01

Prowadź równolegle analizę dostępu pracowników i oszustw klientów.

02

Prawidłowy kontekst płatności nie wystarcza do zatwierdzenia wrażliwej zmiany.

03

Zachowaj koncentrację wydawców w dopasowanym podzbiorze z mianownikiem powiązań urządzeń.

ROZDZIAŁ 10

Regulacje i reakcja instytucji

10

TEN ROZDZIAŁ ODPOWIADA

Które obowiązki zespoły prawne i bezpieczeństwa powinny rozróżniać na dzień odcięcia?

3 kwietnia 2027

termin wdrożenia dla podmiotów objętych wskazanym przepisem przejściowym KSC

10.1 Rozróżniaj podstawy prawne 85
10.2 KSC: rejestracja, wdrożenie i audyt to różne terminy 86
10.3 RODO: dostawca nie zastępuje administratora 86
10.4 DORA: połącz dowody operacyjne i techniczne 86
10.5 Co CISO powinien zrobić teraz 87

ROZDZIAŁ 10

Regulacje i reakcja instytucji

W SKRÓCIE

Nowelizacja KSC obowiązuje, ale rejestracja, wdrożenie i audyt mają różne terminy. Obowiązki RODO nadal dotyczą naruszeń danych osobowych, także u procesorów. Podmioty finansowe potrzebują również procesu raportowania DORA. Jeden incydent może wymagać kilku ocen z różnymi terminami. Potwierdź zakres stosowania, zachowaj chronologię uzyskania wiedzy i przygotuj wstępne zgłoszenia przed kolejnym incydentem u dostawcy.

10.1 Rozróżniaj podstawy prawne

Tabela wskazuje decyzję wymaganą przez każdy instrument. To podsumowanie operacyjne, a nie porada prawna ani ocena stosowania przepisów do konkretnej organizacji.

Instrument	Zakres	Termin	Decyzja operacyjna
Nowelizacja KSC, pozycja 2026/252 [S25][S26]	Podmioty kluczowe i ważne spełniające kryteria ustawowe; istotne są przepisy sektorowe i przejściowe	Obowiązuje od 3 kwietnia 2026; początkowy termin rejestracji 3 października 2026; wskazany termin wdrożenia 3 kwietnia 2027	Ustal status, zachowaj potwierdzenie wpisu i przypisz odpowiedzialność za zabezpieczenia
RODO, artykuły 33–34 [S27]	Administratorzy i procesorzy danych osobowych	Zgłoszenie administratora bez zbędnej zwłoki, w miarę możliwości w ciągu 72 godzin od stwierdzenia, chyba że ryzyko jest mało prawdopodobne	Zapisz moment stwierdzenia, oceń ryzyko i dokonaj wymaganego zgłoszenia
Obowiązek procesora w RODO [S27]	Procesor po stwierdzeniu naruszenia danych osobowych	Zawiadomienie administratora bez zbędnej zwłoki	Dostarcz klientowi informacje potrzebne do jego własnej oceny
DORA [S28]	Podmioty finansowe objęte zakresem, z odpowiednimi wyłączeniami i zasadą proporcjonalności	Stosowane od 17 stycznia 2025	Klasyfikuj incydenty ICT i stosuj właściwą ścieżkę raportowania finansowego

Termin zgłoszenia do organu na podstawie RODO nie rozpoczyna się automatycznie wraz z publikacją zarzutu w prasie. Administrator nie powinien jednak czekać na końcowy raport dostawcy, jeżeli wcześniej uzyskał dostateczną pewność. Zachowaj fakty uzasadniające rzeczywisty moment stwierdzenia naruszenia.

10.2 KSC: rejestracja, wdrożenie i audyt to różne terminy

Szczegółowy harmonogram ministerstwa wskazuje 7 maja–3 października 2026 jako okres samorejestracji podmiotów niewpisywanych z urzędu. Dla podmiotów spełniających wskazane warunki w dniu wejścia ustawy wyznacza 3 kwietnia 2027 na wdrożenie obowiązków i korzystanie z S46 [S26].

Dla nowych podmiotów kluczowych, które nie były operatorami usług kluczowych, termin pierwszego audytu przypada 3 kwietnia 2028. Dotychczasowi operatorzy zachowują cykl audytowy. Wyjaśnienia nie uzasadniają więc twierdzenia, że każda organizacja może odłożyć najbliższy audyt do 2028.

Nowelizacja przewiduje wczesne ostrzeżenie i późniejsze zgłoszenie incydentu, właściwe ścieżki sektorowe oraz przepisy dla dostawców usług zaufania. Prawnicy powinni powiązać te wymagania z przepisami przejściowymi i dotychczasowymi obowiązkami organizacji. Ogólny okres dostosowawczy nie uzasadnia zawieszenia istniejącego procesu reagowania [S25].

Przepisy o karach również wymagają osobnej analizy przejściowej. Artykuł 73 przewiduje dla podmiotu kluczowego limit 10 milionów EUR lub 2% przychodów z działalności, przy zastosowaniu wyższej kwoty. Zawiera też odrębne przepisy dla podmiotów ważnych i poważnych skutków naruszenia [S25].

Harmonogram ministerstwa wskazuje 3 kwietnia 2028 jako początek stosowania przepisów o karach. Data ta nie odracza obowiązków RODO ani DORA. Nie należy traktować możliwej maksymalnej kary jako szacunku prawdopodobnej straty finansowej [S26][S27][S28].

10.3 RODO: dostawca nie zastępuje administratora

Sierpniowe wyjaśnienia UODO dotyczące MyDr wymagają ustalenia, czy incydent obejmuje przetwarzanie związane z konkretnym administratorem. Przypominają o zgłoszeniu organowi oraz zawiadomieniu osób, gdy prawdopodobne jest wysokie ryzyko [S6].

Artykuł 33 RODO dopuszcza przekazywanie informacji etapami, gdy nie można podać ich jednocześnie. Opóźnione zgłoszenie wymaga uzasadnienia. Artykuł 34 zawiera wyjątki od zawiadamiania osób, w tym określone zabezpieczenia lub późniejsze środki usuwające prawdopodobieństwo wysokiego ryzyka [S27].

Warto przygotować zestaw dowodów: przebieg, moment stwierdzenia, kategorie i przybliżone liczby, możliwe konsekwencje, działania zaradcze i punkt kontaktowy. Przybliżone wartości muszą pozostać szacunkami. Liczba wierszy bazy nie powinna stawać się liczbą poszkodowanych osób.

10.4 DORA: połącz dowody operacyjne i techniczne

Serwis DORA prowadzony przez KNF wskazuje rozporządzenie i akty wykonawcze dotyczące klasyfikacji incydentów, zgłaszania, umów i testów. Odporność finansowa wymaga więc współpracy bezpieczeństwa, operacji, zakupów i zgodności [S28].

Bank musi ustalić, czy usługa płatnicza działa, czy incydent ICT spełnia kryteria zgłoszenia i czy obejmuje dane osobowe. To powiązane oceny, lecz każda ma osobne przesłanki prawne. Uspokajający komunikat dostawcy o działaniu usługi nie zamyka wszystkich trzech.

Prowadź jedną chronologię faktów i osobne zapisy decyzji dla każdej ścieżki raportowania. Ogranicza to sprzeczne liczby i daty, zachowując różnice między obowiązkami.

10.5 Co CISO powinien zrobić teraz

Działanie	Właściciel	Dowód wykonania
Potwierdź status KSC, wpis i właściwy okres przejściowy	Dział prawny i sponsor zarządu	Podpisana ocena stosowania i potwierdzenie wpisu albo udokumentowana podstawa wyłączenia
Uzgodnij dotychczasowe audyty z nowym harmonogramem	Audyt i zapewnienie zgodności	Aktualny kalendarz z podstawą prawną każdej daty
Przećwicz incydent procesora przed uzyskaniem pełnych ustaleń	IOD i zakupy	Wstępna ocena ryzyka, zgłoszenie etapowe i żądanie informacji od dostawcy
Połącz oceny DORA i naruszenia danych osobowych	Zgodność finansowa i reagowanie	Jedna chronologia faktów z osobnymi zatwierdzonymi decyzjami
Zweryfikuj właściwy krajowy lub sektorowy kanał zgłoszenia	Reagowanie na incydenty	Sprawdzona lista kontaktów i alternatywna ścieżka przy niedostępności platformy

Eskalacja nie powinna zależeć od jednej skrzynki pocztowej lub jednego administratora. Incydent ePUAP pokazuje potrzebę znajomości alternatywnych kanałów kontaktu i dowodów terminowego złożenia pisma [S31].

NAJWAŻNIEJSZE WNIOSKI

01

Rozróżniaj terminy rejestracji, wdrożenia zabezpieczeń i audytu.

02

Zachowuj ustalenia administratora o momencie stwierdzenia i ryzyku w incydentach dostawców.

03

Uzgadniaj raportowanie cyberbezpieczeństwa, prywatności i finansów na podstawie jednej chronologii faktów.

ROZDZIAŁ 11

Perspektywy

11

TEN ROZDZIAŁ ODPOWIADA

Które oceny mają oparcie w dowodach i co zmieniłoby reakcję?

4

scenariusze planistyczne z wyraźnymi przesłankami

11.1 Kluczowe oceny 89
11.2 Co zmieniłoby ocenę 90
11.3 Scenariusze warunkowe 90
11.4 Unikaj pozornej pewności na dzień odcięcia 90

ROZDZIAŁ 11

Perspektywy

W SKRÓCIE

Dane przechowywane przez dostawców i nadużycia tożsamości są najważniejszymi praktycznymi tematami zweryfikowanych ujawnień. Wpisy ransomware uzasadniają planowanie odtwarzania, lecz nie przewidują, która organizacja ucierpi. Ostatnie ograniczenia usług publicznych pokazują, że przywracanie może wymagać kilku etapów. Stosuj scenariusze warunkowe, przypisz właściciela dowodów i zmieniaj reakcję po uzyskaniu nowych ustaleń o usługach lub kontach.

11.1 Kluczowe oceny

Poziom pewności dotyczy konkretnego twierdzenia. Wysoka pewność, że opublikowano komunikat, nie potwierdza każdego zawartego w nim szacunku.

Ocena	Pewność	Podstawa i ograniczenie	Decyzja
Wspólne oprogramowanie może przenosić ocenę incydentu na wielu niezależnych administratorów	Wysoka	Komunikaty MyDr, FELG i Fakturowni opisują tę zależność; nie każdy klient musi być objęty incydentem [S5][S8] [S10]	Wymagaj informacji dotyczących konkretnego klienta i wskazanego odbiorcy
Prawidłowe dane historyczne mogą uwiarygodnić podszywanie się	Średnia	Ujawnione kategorie obejmują tożsamość, kontakt i kontekst biznesowy; nie wykazano późniejszego wykorzystania w każdym przypadku [S5][S10]	Potwierdzaj uprawnienie przez wcześniej zaufany kanał
Ransomware pozostaje istotnym tematem ciągłości działania	Wysoka dla widoczności, niepewna dla przyszłej częstości	Ransompedia zawiera 56 polskich wpisów; brak incydentów prywatnych i nieopublikowanych [S3]	Odtwórz kluczowy proces z użyciem niezależnych danych dostępowych
Deklaracja grupy nie wystarcza do przypisania zakłóceń usługi	Wysoka	Materiały DDoS i urzędowe relacje o odtwarzaniu opisują inne dowody; nie ustalono ogólnego związku przyczynowego [S30][S31]	Zmierz dostępność i zabezpiecz logi przed wskazaniem przyczyny
Bieżące oferty danych logowania wymagają sprawdzenia kont	Wysoka dla obserwowanego powiązania	Obserwacje dotyczą wybranych domen; własność, aktualność i dostęp są osobnymi pytaniami [S2]	Przed zakłócającym działaniem sprawdź konta, sesje i wcześniejsze działania naprawcze

Oceny nie przewidują częstości ataków, prawdopodobieństwa działań państwowych ani strat finansowych. Dowody nie zapewniają populacji i kontroli potrzebnych do takich szacunków.

11.2 Co zmieniłoby ocenę

Potwierdzenie dotyczące konkretnego klienta pozwoliłoby przejść od zarzutu wobec dostawcy do określonego zakresu incydentu. Zespół tożsamości ustaliłby następnie konta, sesje i kanały odzyskiwania. Zespół prywatności osobno oceniłby informacje dotyczące ludzi.

Nowe ogłoszenie o danych dostępowych lub dostępie uzasadnia weryfikację. Dopasowanie do aktywnego konta i podejrzanej sesji uzasadnia eskalację. Stare hasło, nieaktywne konto lub niepowiązana domena wymagają innej, udokumentowanej decyzji.

Logi dostawcy pokazujące długotrwałe pogorszenie działania zmieniłyby deklarację DDoS w operacyjne dochodzenie dotyczące dostępności. Nie dowodziłyby automatycznie odpowiedzialności deklarującej grupy. Sama zbieżność czasu jest słabsza od dowodu technicznego.

Zmienione zalecenia producenta dotyczące poprawionych wersji zmieniłyby plan aktualizacji. Przykład RouterOS pokazuje potrzebę sprawdzania bieżącego biuletynu, zamiast zakładania, że pierwsza wskazana wersja pozostaje zalecanym celem [S20].

11.3 Scenariusze warunkowe

To założenia planistyczne. Nie są prognozami zdarzeń ani twierdzeniami, że wskazana organizacja obecnie nie stosuje danego zabezpieczenia.

Scenariusz	Przesłanka	Pierwsza reakcja	Dowód wykonania
Procesor ujawnia dostęp do rekordów klientów	Dostawca potwierdza objęcie Twojego konta lub gabinetu	Zachowaj komunikat; ustal kategorie danych, moment stwierdzenia i procesy	Zakres dotyczący administratora i zatwierdzone decyzje o zgłoszeniach
Po komunikacie pojawia się wiarygodna zmiana faktury	Dostawca żąda nowego rachunku, podając rzeczywiste dane faktury	Wstrzymaj zmianę i zadzwoń do wcześniej znanej osoby	Niezależne potwierdzenie i zapisana decyzja płatnicza
Usługa publiczna ogranicza dostęp po incydencie	Użytkownicy nie mogą złożyć kluczowego pisma elektronicznie	Uruchom ustaloną alternatywę i zachowaj dowód złożenia	Akceptacja właściciela procesu, że alternatywa działa
Grupa o politycznej narracji wskazuje Twoją witrynę	Pojawia się deklaracja z listą celów lub zrzutem dostępności	Potwierdź stan usługi z dostawcą i w razie potrzeby uruchom ochronę	Zapisane pomiary działania i komunikat oparty na faktach

11.4 Unikaj pozornej pewności na dzień odcięcia

Ostatnie dni nie tworzą pełnego miesiąca. Ujawnienie może nastąpić wiele tygodni po dostępie, co pokazuje chronologia uczelni. Późniejszy komunikat może aktualizować wcześniejszy incydent bez tworzenia nowego przypadku [S41].

Te ograniczenia dotyczą też porównań. Polski wynik za część 2026 i wynik za cały 2025 obejmują różne okresy. Różnica opisuje widoczność, a nie zmierzone roczne tempo wzrostu. Państwa porównawcze różnią się także wielkością gospodarki i praktyką ujawnień [S3].

Kraje do porównania wybrano jako przykłady wyłącznie w celu przedstawienia kontekstu; ich wybór nie oznacza rankingu ani oceny politycznej.

Traktuj perspektywy jako ramy decyzji podlegające aktualizacji. Każdy zespół powinien znać fakt uruchamiający dochodzenie, ograniczenie dostępu oraz przejście od odtwarzania do akceptacji biznesowej.

NAJWAŻNIEJSZE WNIOSKI

01

Każdej ocenie przypisz granicę dowodową i sygnał zmiany.

02

Uruchamiaj konkretne działania na podstawie sygnałów dostawcy, tożsamości i dostępności.

03

Aktualizuj ocenę po potwierdzeniu, nie licząc kolejnych komunikatów jako nowych incydentów.

ROZDZIAŁ 12

Plan działania

12

TEN ROZDZIAŁ ODPOWIADA

Kto powinien działać przez 30, 60 i 90 dni oraz co potwierdzi wykonanie?

90 dni

na sprawdzenie decyzji dotyczących tożsamości, dostawców i odtwarzania

12.1 Plan na 30/60/90 dni 93
12.2 Odpowiedzialność według ról 95
12.3 Praktyczna karta wykonania 96
12.4 Jak może pomóc Brandefense 97

ROZDZIAŁ 12

Plan działania

W SKRÓCIE

Zacznij od zależności mogących ujawnić rekordy lub zatrzymać kluczową pracę: tożsamości, wspólnego oprogramowania, płatności i odtwarzania. Wyznacz właścicieli biznesowych i technicznych. Testuj zabezpieczenia na danych syntetycznych i w uzgodnionych ćwiczeniach. Zamykaj działanie po wykazaniu właściwej decyzji lub działania usługi, a nie po napisaniu procedury. Ustal priorytety na podstawie poniższego planu.

12.1 Plan na 30/60/90 dni

Każde działanie wynika z przesłanki lub zweryfikowanego przypadku. Cele są proponowanymi założeniami zarządczymi, a nie pomiarem wyników polskich organizacji.

1Dni 1–30

Dla każdego kluczowego procesu wskaż dostawcę tożsamości, procesora, kontakt wsparcia i zależności odtwarzania

WŁAŚCICIEL

Operacje biznesowe i architektura

DOWÓD WYKONANIA

Zatwierdzony rejestr zależności z odpowiedzialnym właścicielem usługi

Jeśli komunikat dostawcy obejmuje Twoje konto, zachowaj go i ustal konkretny zakres danych [S5][S8][S10]

WŁAŚCICIEL

Zakupy i IOD

DOWÓD WYKONANIA

Udokumentowany moment stwierdzenia, kategorie danych i wstępna ocena zgłoszenia

Przy ogłoszeniu dostępu lub danych dostępowych sprawdź status konta, aktualność, sesje i wcześniejsze działania

WŁAŚCICIEL

Zespół tożsamości i SOC

DOWÓD WYKONANIA

Decyzja dla każdego sygnału i eskalacja potwierdzonego nieuprawnionego użycia

Jeśli mogły zostać ujawnione faktury lub dane kontrahentów, niezależnie potwierdzaj zmiany odbiorcy płatności [S10]

WŁAŚCICIEL

Finanse i przeciwdziałanie oszustwom

DOWÓD WYKONANIA

Zatrzymane syntetyczne oszustwo i poprawnie wykonana prawidłowa dyspozycja

Porównaj wersje produktów brzegowych z aktualnymi zaleceniami producenta i CERT [S20][S23]

WŁAŚCICIEL
Infrastruktura

DOWÓD WYKONANIA
Dowody wersji, zatwierdzone wyjątki i właściciel każdej zaległości

Potwierdź rejestrację KSC i właściwe terminy wdrożenia [S25][S26]

WŁAŚCICIEL
Dział prawny i sponsor zarządu

DOWÓD WYKONANIA
Podpisana ocena stosowania i finansowanie pozostałych obowiązków

2Dni 31–60

Nadaj pierwszeństwo MFA odpornemu na phishing dla kont uprzywilejowanych i o dużym wpływie [S14]

WŁAŚCICIEL
Zespół tożsamości i właściciele biznesowi

DOWÓD WYKONANIA
Pokrycie względem uzgodnionego wykazu kont i sprawdzona ścieżka odzyskiwania

Przejrzyj podejrzane logowania, nowe reguły pocztowe, zgody tokenowe i nietypowe eksporty masowe

WŁAŚCICIEL
SOC i poczta

DOWÓD WYKONANIA
Uzgodniony test dociera do analityka z kontekstem konta i sesji

Przy mobilnych płatnościach oceń instalację spoza sklepu, uprawnienia dostępności i płatności operatorskie [S15][S16]

WŁAŚCICIEL
Urządzenia końcowe i przeciwdziałanie oszustwom

DOWÓD WYKONANIA
Kontrolowany test jest blokowany lub wykrywany; wsparcie ma bezpieczny scenariusz rozmowy

Odtwórz kluczową usługę z chronionej kopii i niezależnymi danymi dostępowymi [S35]

WŁAŚCICIEL
Infrastruktura i właściciel usługi

DOWÓD WYKONANIA
Działający proces, kontrola integralności i akceptacja biznesowa

Przećwicz incydent procesora przy niepełnych ustaleniach [S6][S27]

WŁAŚCICIEL
IOD, zakupy i reagowanie

DOWÓD WYKONANIA
Wstępne zgłoszenie, wykaz pytań i termin aktualizacji

Przećwicz niedostępność platformy składania pism lub portalu klienta [S31][S34]

WŁAŚCICIEL
Operacje i dział prawny

DOWÓD WYKONANIA
Działająca alternatywa, zachowane terminy i sprawdzony kanał komunikacji

3Dni 61–90

Przeprowadź ćwiczenie DDoS i publicznej deklaracji, oddzielając pomiary dostawcy od twierdzeń grupy [S30]

WŁAŚCICIEL
Sieć, komunikacja i SOC

DOWÓD WYKONANIA
Uruchomienie ochrony, komunikaty oparte na faktach i dowody działania usługi

W procesach przemysłowych sprawdź odtwarzanie łączności terenowej i zdalnego zarządzania [S18]

WŁAŚCICIEL
Inżynieria OT i operacje

DOWÓD WYKONANIA
Bezpieczny proces, zatwierdzona konfiguracja i niezależny dostęp odtworzeniowy

Sprawdź eskalację u dostawcy poza zwykłymi godzinami pracy

WŁAŚCICIEL
Zakupy i reagowanie

DOWÓD WYKONANIA
Wskazany pracownik dostawcy przekazuje informację w terminie umownym

Przedstaw kierownictwu pozostałe luki zabezpieczeń i dowodów

WŁAŚCICIEL
CISO i właściciele usług

DOWÓD WYKONANIA
Zaakceptowane ryzyka, właściciele i terminy zakończenia

12.2 Odpowiedzialność według ról

Zarząd i sponsor wykonawczy. Zatwierdź priorytety usług i ryzyko rezydualne. Pytaj, jaką transakcję biznesową odtworzono w teście, który dostawca potrafi wskazać objęte dane i kto może zatwierdzić ponowne uruchomienie usługi.

CISO i reagowanie na incydenty. Prowadź zapis decyzji łączący sygnał z jego weryfikacją i reakcją. Zarzut, urzędowe ujawnienie i zdarzenie zaobserwowane wewnętrznie zachowuj osobno, dopóki dowody nie uzasadnią ich powiązania.

Tożsamość i poczta. Oceniaj razem dostęp uprzywilejowany, kanały odzyskiwania i aktywne sesje. Sama zmiana hasła może pozostawić inne ścieżki dostępu. Dla kont o dużym wpływie wybieraj metody odporne na phishing i sprawdzaj odzyskiwanie przez wsparcie.

SOC i wywiad o zagrożeniach. Zachowuj pierwszą obserwację, aktualizacje publiczne i odpowiednie logi. Nie zamykaj zarzutu tylko dlatego, że usługa obecnie działa. Oznaczenie kraju, zrzut ekranu lub powtórzony tytuł zbioru również nie dowodzą włamania.

Infrastruktura i OT. Utrzymuj zaufaną konfigurację oraz dostęp odtworzeniowy. Porównuj zainstalowane wydanie z aktualnym biuletynem, a po zmianach sprawdzaj usługę. W środowisku przemysłowym uwzględnij łączność terenową i bezpieczne działanie procesu w odbiorze.

Finanse i przeciwdziałanie oszustwom. Traktuj prawidłowe dane faktury, tożsamości lub zdrowia jako kontekst, który oszust może już znać. Nietypowe instrukcje potwierdzaj kanałem ustalonym przed żądaniem. Zapewnij konsultantom bezpieczny sposób zakończenia podejrzanej rozmowy i ponownego kontaktu z klientem.

Prawo, prywatność i zakupy. Ustal role administratora i procesora przed incydentem. Podczas reakcji zapisuj moment stwierdzenia, ocenę ryzyka i decyzje o zawiadomieniu. Wymagaj przydatnych informacji etapowych i uzasadniaj zastosowanie każdej ścieżki zgłoszenia.

12.3 Praktyczna karta wykonania

Karta ocenia zdolność podejmowania i wykazywania wymaganych decyzji. Nie zakłada, że pojedyncze zabezpieczenie eliminuje daną ścieżkę ataku.

Pytanie	Proponowany cel	Dowód
Czy kluczowe procesy mają odpowiedzialnych właścicieli?	Każdy proces w zatwierdzonym wykazie usług kluczowych	Właściciel i zapis zależności
Czy sygnały tożsamości otrzymują uzasadnioną decyzję?	Każdy sygnał przyjęty do kolejki weryfikacyjnej	Ocena aktualności, konta, sesji i wcześniejszych działań
Czy incydent procesora uruchamia właściwy termin?	Każde ćwiczenie zawiera zapis momentu stwierdzenia	Chronologia, ocena ryzyka i decyzja o zgłoszeniu
Czy użytkownicy o dużym wpływie są chronieni przed przekazywaniem danych logowania?	Pokrycie MFA odpornym na phishing względem uzgodnionego wykazu	Wykaz metod i kontrolowany test logowania
Czy płatność wytrzyma przekonujące podszywanie się?	Każda testowana zmiana odbiorcy jest niezależnie sprawdzana	Zapis oddzwonienia i zatwierdzenia płatności
Czy odtwarzanie działa po utracie administracji produkcyjnej?	Każdy wybrany proces kluczowy przechodzi ćwiczenie	Zapis odtworzenia, integralności i akceptacji biznesowej

Potwierdzanie numerem nie jest w tej karcie uznawane za MFA odporne na phishing. Usprawnienie przejściowe należy tak nazwać. Czerwcowa kampania wyraźnie obejmuje wyłudzanie jednorazowych kodów uwierzytelniania [S14].

12.4 Jak może pomóc Brandefense

Wykorzystaj zewnętrzne informacje o zagrożeniach do skierowania ogłoszenia lub sygnału o danych dostępowych do właściwego właściciela. Połącz tę kolejkę z własnymi dowodami dotyczącymi tożsamości, urządzeń, dostawców i usług. Wynikiem powinna być uzasadniona decyzja, a nie większa liczba alertów.

Raport pokazuje to podejście za pomocą zanonimizowanych kart, odrębnych populacji źródłowych i działań z warunkiem zakończenia. Rozdział ekspozycji dodaje bieżące oferty, powiązania urządzeń i danych logowania oraz krajową ocenę Atlas wybranego portfela. Zweryfikuj sygnały wobec własnych kont i usług.

Omów monitoring i weryfikację istotne dla Twojej organizacji: Umów prezentację.

NAJWAŻNIEJSZE WNIOSKI

01

Każdemu priorytetowi przypisz właściciela biznesowego i obserwowalny dowód wykonania.

02

Testuj wspólnie zgłoszenie dostawcy, potwierdzanie płatności i niezależne odtwarzanie.

03

Zamykaj działania na podstawie wykazanych decyzji i działających usług.

ZAŁĄCZNIKI

Załączniki

A–D

TEN ROZDZIAŁ ODPOWIADA

Jakie populacje, daty i granice pewności obowiązują w raporcie?

4

rodzaje dowodów zachowane oddzielnie

Dodatek A. Metoda i granice dowodowe 99

Dodatek B. Rejestr dowodów 102

Dodatek C. Źródła 103

Dodatek D. Słownik 107

Dodatek A. Metoda i granice dowodowe

Kraje do porównania wybrano jako przykłady wyłącznie w celu przedstawienia kontekstu; ich wybór nie oznacza rankingu ani oceny politycznej.

A.1 Zakres badania

Raport dotyczy Polski, kod PL. Okres dat wpisów to 1 stycznia–22 listopada 2026. Źródła publiczne i obserwacje pasywne odczytano 22 listopada. Ostatnia aktywność obejmuje 9–22 listopada. Ostatni dzień i listopad są częściowe.

Odbiorcy to kierownictwo bezpieczeństwa, SOC, właściciele tożsamości i infrastruktury, zespoły oszustw, prawa i zakupów. Raport wspiera decyzje dotyczące zakresu dostawcy, uprawnień kont, zgłoszeń, odtwarzania i komunikacji.

Źródła obejmują wpisy podziemia gromadzone przez Odin by Brandefense, publiczne wpisy ransomware, obserwacje DNS i TLS, komunikaty urzędowe, akty prawne i publiczne badania. Wnioski zachowują zakres właściwy źródłu.

A.2 Wpisy i ogłoszenia

Populacja publikacji obejmuje 118 390 wpisów związanych z krajem. Zachowana treść zawiera 119 484 odrębnych wpisów, w tym 1 434 forumowych. To różne populacje. Treść jest częściowa i nie służy do estymacji krajowej przestępczości [S1].

Ocena treści w rozdziale 4 dotyczy 43 320 potencjalnie istotnych wpisów wśród 118 387 zachowanych wpisów związanych z krajem. Kategorie nakładają się. Nie mierzy odrębnych ofert, sprzedawców, transakcji ani incydentów.

Ogłoszenie może dotyczyć starszych informacji. Deklarowana data eksportu nie jest zweryfikowaną datą włamania. Podobny tekst uzasadnia ciągłość reklamy bez ustalania tożsamości pliku lub wspólnego operatora. Nie pozyskiwano plików z odnośników ani nie testowano oferowanego dostępu.

A.3 Wybrane organizacje i obserwacje pasywne

Prywatna lista kandydatów obejmuje 250 domen. Obserwacje ekspozycji obejmują 250; pasywne obejmują 241. Wybór jest celowy, a tożsamość kandydatów wymaga weryfikacji. Wyniki opisują więc domeny związane z listą, a nie reprezentatywną próbę kraju [S2].

DMARC opisuje żądania polityk, a nie pełne egzekwowanie. Obserwacja DKIM i rekordu delegacji nie ustala całego podpisywania lub walidacji DNSSEC. TLS i strony zachowują własne mianowniki rozstrzygających wyników lub odpowiedzi.

Krajowa ocena Atlas wynosi 51 na 100. Publikuje się wyłącznie tę ocenę krajową. Tabele sektorowe zawierają liczby sygnałów. Dane ekspozycji odczytano 21 listopada 2026; dodatkowe liczby źródłowe i obserwacje pasywne 22 listopada 2026.

Powiązania urządzeń i danych logowania mogą obejmować stare rekordy. Wzmianki obejmują poprzednie 365 dni; domeny podobne 30 dni. Powiązania nakładają się między źródłami i domenami. Miary nie ustalają odrębnych osób, aktywnych danych logowania lub włamania do organizacji [S2].

A.4 Wpisy ransomware

Ransompedia dostarcza zbiór dla Polski i czterech partnerów regionalnych. Okres opiera się na publikacji wpisu lub dacie zastępczej źródła, gdy publikacji brak. Nie ustala dat włamania [S3].

Etykiety kraju i grupy pochodzą ze źródła. Wpis może powtarzać organizację lub dotyczyć związku międzynarodowego. Raport nie potwierdza niezależnie wszystkich krajów, szyfrowania i odrębności ofiar.

Okres 2026 i cały 2025 mają różną długość. Gospodarki i praktyki ujawnień także się różnią. Liczby porównują widoczność, a nie ryzyko państw lub zmierzone roczne tempo wzrostu.

A.5 Materiały kartowe

Wyniki dotyczą tylko kart widocznych jawnie w zebranych wpisach. Brandefense wykrywa skradzione karty wieloma innymi metodami poza raportem. Liczba 455 kart związanych z Polską nie mierzy krajowej kradzieży, ważności ani strat [S4].

Wydanie publiczne zawiera wyłącznie liczby zbiorcze. Nie publikuje numerów kart, indywidualnych płatności ani rankingu wydawców. Połączony widok ekspozycji wydawców obejmuje wybrany podzbiór banków; pozostałe usługi finansowe pozostają w szerszym portfelu sektora.

A.6 Weryfikacja podatności

Każdy CVE przywołany w raporcie lub tytule cytowanego materiału sprawdzono w NVD. Tabela rozróżnia pierwsze poprawki konkretnego problemu od szerszych bieżących zaleceń. Przed aktualizacją sprawdź edycję i kanał [S20][S21][S22][S23][S24][S52][S53].

CVE	Wersje podatne	Zweryfikowane działanie
CVE-2026-67279 i CVE-2026-86060	RouterOS 6.0 przed 6.49.21; 7.0 przed 7.23.4; 7.24 przed 7.24.2	NVD wskazuje pierwsze poprawki 6.49.21, 7.23.4 i 7.24.2. Szersze zalecenia CERT wskazują stable 7.24.3, long-term 7.23.6 lub RouterOS 6.49.21, albo późniejsze właściwe wydania
CVE-2026-87850	nVision poniżej 18 według CERT Polska	Wersja 18; NVD także wskazuje tę poprawkę
CVE-2026-21509	Rodziny Office 2016, 2019, Microsoft 365 Apps i LTSC 2021/2024 wymienione w NVD	Microsoft wskazuje Office 2016 kompilacja 16.0.5539.1001 i Office 2019 kompilacja 16.0.10417.20095. Microsoft 365 Apps, Office 2021 i nowsze otrzymują ochronę usługową wymagającą restartu aplikacji

Tabela służy obronie i wersjom, a nie opisowi wykorzystania. Komunikat podatności nie dowodzi ataku na wybraną polską organizację. Raport nie zawiera instrukcji ofensywnych ani działającego kodu.

A.7 Incydenty publiczne i kampanie

Badanie obejmowało okres raportu i oficjalne materiały CERT Polska, CSIRT GOV/ABW, CSIRT MON, UODO, ministerstwa oraz policji. Zakres pozostaje częściowy; brak opisu nie dowodzi braku incydentu.

Miesięczne podsumowania opisują wybrane kampanie i mogą powtarzać motyw. Data publikacji lub zmiany komunikatu nie oznacza automatycznie daty incydentu. Historyczne zdarzenia ujawnione w 2026 pozostają kontekstem historycznym.

Publiczny rejestr stosuje role ogólne poza zatwierdzonymi nazwami potwierdzonymi oficjalnie i szeroko opisywanymi. Nie publikuje się adresów źródeł identyfikujących nieujawniane organizacje. Nie publikuje się danych osobowych, kontaktów ani punktów końcowych ofiar.

A.8 Pewność i neutralność polityczna

Obserwacja oznacza zachowany materiał lub pomiar. Twierdzenie przestępcze pozostawia zasadniczy zarzut niezweryfikowany. Relacja oficjalna ustala treść wypowiedzi źródła w jego zakresie. Interpretacja analityczna łączy te fakty z decyzją.

Wysoka pewność dotyczy konkretnego twierdzenia, a nie wszystkich wypowiedzi aktora. Wpis nie dowodzi szyfrowania, stare dane logowania nie oznaczają aktualnego dostępu, a powiązanie nie ustala własności. Niezweryfikowane nie znaczy fikcyjne.

Przypisania państwowe, orientacja polityczna i nazwy kampanii pozostają ocenami źródeł. Język nie ustala narodowości ani sponsora. Autorzy nie zajmują stanowiska wobec władz, Rosji, Białorusi, Ukrainy, wyborów, terytorium i polityki międzynarodowej.

Dodatek B. Rejestr dowodów

Karty zawierają krótkie zanonimizowane fragmenty i oddzielają ofertę od nieustalonych faktów. Daty wpisów nie ustalają dat włamania. Mapowanie źródeł pozostaje prywatne.

Karta	Data	Miejsce	Alias	Język	Rozdział
B01	2026-02-27	Forum	metadata	Angielski	4
B02	2026-08-21	Forum	updap	Angielski	4
B03	2026-11-15	Forum	Sophia	Angielski	4
B04	2026-05-11	Forum	MDGhost	Angielski	4
B05	2026-01-05	Forum	daghetiaw	Angielski	4
B06	2026-02-02	Forum	Robert2025	Angielski	4
B07	2026-09-13	Telegram	NoName057(16)	Angielski	6
B08	2026-11-16	Forum	kenpiraa	Angielski	4
B09	2026-08-23	Forum	updap	Angielski	4
B10	2026-04-27	Forum	xcgtyrewty	Angielski	4
B11	2026-11-13	Forum	thisversace	Angielski	4
B12	2026-03-20	Forum	Katarinka	Angielski	4
B13	2026-04-06	Forum	Katarinka	Angielski	4
B14	2026-04-06	Forum	KazeFreak	Angielski	4
B15	2026-05-16	Forum	org1877	Angielski	4
B16	2026-11-12	Forum	Suction19213821	Angielski	6
B17	2026-01-23	Forum	Spirigatito	Angielski	5

Siedem ofert A–F i U odpowiada B01–B06 i B12. B17 wspiera przypadek V; oficjalny komunikat i większe sumy sprzedawcy zachowują odrębne zakresy. B07 jest wzmianką o kampanii, a B08–B11 i B13–B16 dodatkowymi obserwacjami. Piętnaście przypadków prowadzonych od oficjalnych komunikatów G–T i V stanowi odrębne pozycje. Przypadek V porównuje także powiązane ogłoszenie.

Dodatek C. Źródła

Każde źródło zewnętrzne odczytano dla odpowiedniego fragmentu. Data weryfikacji oznacza sprawdzenie źródła, a nie niezależne potwierdzenie jego wszystkich twierdzeń. Dane własne odnoszą się do zachowanych dowodów i agregatów, nie zewnętrznie odtwarzalnego spisu krajowego.

S1: Odin by Brandefense, Retained Poland posts and aggregate observations. https://brandefense.io/. Own evidence retained privately; publisher URL is not a public copy of the raw evidence. Zweryfikowano 22 listopada 2026.

S2: Odin by Brandefense, Selected-domain Atlas exposure and passive observations. https://brandefense.io/. Own evidence retained privately; publisher URL is not a public copy of the raw evidence. Zweryfikowano 22 listopada 2026.

S3: Odin by Brandefense, Ransomware listing snapshot, Poland and regional peers. https://brandefense.io/. Own evidence retained privately; publisher URL is not a public copy of the raw evidence. Zweryfikowano 22 listopada 2026.

S4: Odin by Brandefense, Pooled card observations in retained posts. https://brandefense.io/. Own evidence retained privately; publisher URL is not a public copy of the raw evidence. Zweryfikowano 22 listopada 2026.

S5: Ministry of Digital Affairs, Joint cyber operations centre statement on MyDr. https://www.gov.pl/web/cyfryzacja/komunikat-po-spotkaniu-polaczonego-centrum-operacyjnego-cyberbezpieczenstwa. Zweryfikowano 22 listopada 2026.

S6: UODO, Controller obligations after a processor data incident. https://uodo.gov.pl/pl/138/4538. Zweryfikowano 22 listopada 2026.

S7: UODO, Medical-software incident and planned inspection. https://uodo.gov.pl/pl/138/4585. Zweryfikowano 22 listopada 2026.

S8: FELG Software, Security incident and updates. https://status.felg.cloud/incydent. Zweryfikowano 22 listopada 2026.

S9: AHA / Health-ISAC, Bulletin on the FELG Software incident. https://www.aha.org/h-isac-white-reports/2026-10-02-threat-bulletin-tlp-white-data-breach-polish-dental-software-vendor-felg-software-felg-dent. Zweryfikowano 22 listopada 2026.

S10: Fakturownia, Security incident, expanded notice. https://fakturownia.pl/incydent-eng. Zweryfikowano 22 listopada 2026.

S12: enel-med, Patient-data incident notice, 27 September. https://enel.pl/komunikat/. Zweryfikowano 22 listopada 2026.

S14: CERT Polska, UNC1151/Ghostwriter Gmail phishing campaign. https://cert.pl/posts/2026/06/UNC1151-kampania-gmail/. Zweryfikowano 22 listopada 2026.

S15: CERT Polska, Analysis of Polish-targeted mobile toll fraud. https://cert.pl/posts/2026/09/analiza-tollfraud/. Zweryfikowano 22 listopada 2026.

S16: CERT Polska, FvncBot campaign analysis. https://cert.pl/posts/2026/03/analiza-fvncbot/. Zweryfikowano 22 listopada 2026.

S18: CERT Polska, Energy-sector incident of 29 December 2025, reported in January 2026. https://cert.pl/posts/2026/01/raport-incydent-sektor-energii-2025/. Zweryfikowano 22 listopada 2026.

S20: CERT Polska, RouterOS exploitation advisory and current product guidance. https://cert.pl/posts/2026/09/podatnosci-w-mikrotik-routeros-aktywnie-wykorzystywane/. Zweryfikowano 22 listopada 2026.

S21: NVD, CVE-2026-67279. https://nvd.nist.gov/vuln/detail/CVE-2026-67279. Full NVD response retained privately; affected configurations and fixes checked against cited advisories. Zweryfikowano 22 listopada 2026.

S22: NVD, CVE-2026-86060. https://nvd.nist.gov/vuln/detail/CVE-2026-86060. Full NVD response retained privately; affected configurations and fixes checked against cited advisories. Zweryfikowano 22 listopada 2026.

S23: CERT Polska, Axence nVision advisory. https://cert.pl/posts/2026/11/CVE-2026-87850/. Zweryfikowano 22 listopada 2026.

S24: NVD, CVE-2026-87850. https://nvd.nist.gov/vuln/detail/CVE-2026-87850. Full NVD response retained privately; affected configurations and fixes checked against cited advisories. Zweryfikowano 22 listopada 2026.

S25: Polish legal publication service, KSC amendment, Act of 23 January 2026, item 252. https://eli.gov.pl/api/acts/DU/2026/252/text.pdf. Zweryfikowano 22 listopada 2026.

S26: Ministry of Digital Affairs, KSC implementation timetable. https://www.gov.pl/web/cyfryzacja/nowelizacja-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-ksc--najwazniejsze-terminy. Zweryfikowano 22 listopada 2026.

S27: EUR-Lex, GDPR, Articles 33 and 34. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng. Zweryfikowano 22 listopada 2026.

S28: KNF, DORA regulation and implementing instruments. https://www.knf.gov.pl/dla_rynku/dora. Zweryfikowano 22 listopada 2026.

S29: DataReportal, Digital 2027: Poland, published November 2026. https://datareportal.com/reports/digital-2027-poland. Zweryfikowano 22 listopada 2026.

S30: ZeroFox, DDoS claims research, including January Poland observations. https://www.zerofox.com/intelligence/flash-report-ddos-attacks-target-spanish-government-websites/. Zweryfikowano 22 listopada 2026.

S31: Ministry of Digital Affairs, Full ePUAP restoration notice, 19 November. https://www.gov.pl/web/cyfryzacja/epuap-ponownie-dziala-w-pelnym-zakresie. Zweryfikowano 22 listopada 2026.

S33: Ministry of Culture, SOP security incident notice. https://www.gov.pl/web/kultura/komunikat-dotyczacy-naruszenia-bezpieczenstwa-danych-w-systemie-sop. Zweryfikowano 22 listopada 2026.

S34: Ministry of Culture, Programme timetable and SOP recovery update. https://www.gov.pl/web/kultura/komunikat-dotyczacy-opoznienia-ogloszenia-naboru-do-programow-ministra-2027n. Zweryfikowano 22 listopada 2026.

S35: Centre for e-Health, Sector response and regional-hospital recovery account. https://cez.gov.pl/pl/page/o-nas/aktualnosci/lepsza-wspolpraca-wieksze-cyberbezpieczenstwo. Zweryfikowano 22 listopada 2026.

S41: University of Warsaw, Personal-data breach notice and updated chronology. https://www.uw.edu.pl/komunikat-w-sprawie-naruszenia-ochrony-danych-osobowych/. Zweryfikowano 22 listopada 2026.

S43: National Centre for Nuclear Research, Blocked attempted IT attack, 12 March statement. https://www.ncbj.gov.pl/aktualnosci/udaremnienie-cyberataku-na-narodowe-centrum-badan-jadrowych. Zweryfikowano 22 listopada 2026.

S44: ESET, Webworm: New burrowing techniques, chiefly 2025 activity. https://www.welivesecurity.com/en/eset-research/webworm-new-burrowing-techniques/. Zweryfikowano 22 listopada 2026.

S45: Autopay, Data-security incident statement. https://autopay.pl/baza-wiedzy/aktualnosci/informacja-autopay-s-a-dotyczaca-zdarzenia-zwiazanego-z-bezpieczenstwem-danych. Zweryfikowano 22 listopada 2026.

S46: PRNews, Autopay access incident, 14 November reporting. https://prnews.pl/cyberatak-na-autopay-nieuprawniony-dostep-do-czesci-danych-o-platnosciach-501801. Zweryfikowano 22 listopada 2026.

S47: MITRE ATT&CK, Spearphishing Link. https://attack.mitre.org/techniques/T1566/002/. Zweryfikowano 22 listopada 2026.

S48: MITRE ATT&CK, Multi-Factor Authentication Interception. https://attack.mitre.org/techniques/T1111/. Zweryfikowano 22 listopada 2026.

S49: MITRE ATT&CK, Valid Accounts. https://attack.mitre.org/techniques/T1078/. Zweryfikowano 22 listopada 2026.

S50: MITRE ATT&CK, Remote Email Collection. https://attack.mitre.org/techniques/T1114/002/. Zweryfikowano 22 listopada 2026.

S51: DKWOC, Crafty Leshy targeted document campaign analysis. https://www.wojsko-polskie.pl/woc/articles/aktualnosci-w/cve-2026-21509-opis-podatnosci-i-przeglad-zaobserwowanej-kampanii/. Exact publication date not exposed; observation on 30 January 2026 is stated in the primary text. Zweryfikowano 22 listopada 2026.

S52: NVD, CVE-2026-21509. https://nvd.nist.gov/vuln/detail/CVE-2026-21509. Full NVD response retained privately; affected configurations and fixes checked against cited advisories. Zweryfikowano 22 listopada 2026.

S53: Microsoft MSRC, Office security feature bypass advisory and fixed builds. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21509. Zweryfikowano 22 listopada 2026.

S54: Chief Sanitary Inspectorate, Food cold-chain infrastructure warning. https://www.gov.pl/web/gis/komunikat-glownego-inspektora-sanitarnego-w-sprawie-potencjalnych-zagrozen-zwiazanych-z-atakami-na-infrastrukture-lancucha-chlodniczego-w-przemysle-spozywczym. Zweryfikowano 22 listopada 2026.

S55: PAP, CERT statement on a Polish refrigeration-device incident. https://www.pap.pl/aktualnosci/cert-polska-w-kraju-doszlo-do-cyberataku-na-urzadzenie-chlodnicze. Zweryfikowano 22 listopada 2026.

S56: Healthcare provider, Ransomware notice concerning 13 March. Source URL withheld to protect the organisation; underlying primary notice retained privately. Zweryfikowano 22 listopada 2026.

S57: Healthcare provider, Ransomware notice concerning 24 March. Source URL withheld to protect the organisation; underlying primary notice retained privately. Zweryfikowano 22 listopada 2026.

S58: Healthcare provider, Ransomware notice concerning 31 March. Source URL withheld to protect the organisation; historical adjacent notice is separate. Zweryfikowano 22 listopada 2026.

S61: CERT Polska, Monthly threat summary, 2026-01. https://cert.pl/uploads/docs/Podsumowanie_CERT_Polska_2026_01.pdf. Monthly campaign observations; recurring patterns are not separate incident counts. Zweryfikowano 22 listopada 2026.

S62: CERT Polska, Monthly threat summary, 2026-02. https://cert.pl/uploads/docs/Podsumowanie_CERT_Polska_2026_02.pdf. Monthly campaign observations; recurring patterns are not separate incident counts. Zweryfikowano 22 listopada 2026.

S63: CERT Polska, Monthly threat summary, 2026-03. https://cert.pl/uploads/docs/Podsumowanie_CERT_Polska_2026_03.pdf. Monthly campaign observations; recurring patterns are not separate incident counts. Zweryfikowano 22 listopada 2026.

S64: CERT Polska, Monthly threat summary, 2026-04. https://cert.pl/uploads/docs/Podsumowanie_CERT_Polska_2026_04.pdf. Monthly campaign observations; recurring patterns are not separate incident counts. Zweryfikowano 22 listopada 2026.

S65: CERT Polska, Monthly threat summary, 2026-05. https://cert.pl/uploads/docs/Podsumowanie_CERT_Polska_2026_05.pdf. Monthly campaign observations; recurring patterns are not separate incident counts. Zweryfikowano 22 listopada 2026.

S66: CERT Polska, Monthly threat summary, 2026-06. https://cert.pl/uploads/docs/Podsumowanie_CERT_Polska_2026_06.pdf. Monthly campaign observations; recurring patterns are not separate incident counts. Zweryfikowano 22 listopada 2026.

S67: CERT Polska, Monthly threat summary, 2026-07. https://cert.pl/uploads/docs/Podsumowanie_CERT_Polska_2026_07.pdf. Monthly campaign observations; recurring patterns are not separate incident counts. Zweryfikowano 22 listopada 2026.

S68: CERT Polska, Monthly threat summary, 2026-08. https://cert.pl/uploads/docs/Podsumowanie_CERT_Polska_2026_08.pdf. Monthly campaign observations; recurring patterns are not separate incident counts. Zweryfikowano 22 listopada 2026.

S69: CERT Polska, Monthly threat summary, 2026-09. https://cert.pl/uploads/docs/Podsumowanie_CERT_Polska_2026_09.pdf. Monthly campaign observations; recurring patterns are not separate incident counts. Zweryfikowano 22 listopada 2026.

S70: CERT Polska, Monthly threat summary, 2026-10. https://cert.pl/uploads/docs/Podsumowanie_CERT_Polska_2026_10.pdf. Monthly campaign observations; recurring patterns are not separate incident counts. Zweryfikowano 22 listopada 2026.

S71: Industrial company, Ransomware notice and update history. Source URL withheld to protect the organisation; history gives first publication 3 November and expansion 19 November; heading gives 10 November. Zweryfikowano 22 listopada 2026.

S72: Żabka, Information about the technical-resource access incident. https://www.zabka.pl/informacja-dla-klientow-w-zwiazku-z-incydentem-w-obszarze-bezpieczenstwa-systemu-informatycznego/. Zweryfikowano 22 listopada 2026.

S73: ZUS, Login to PUE/eZUS restored. https://www.zus.pl/o-zus/komunikaty/komunikaty-techniczne/-/asset_publisher/komunikatytechniczne/content/id/14328424. Zweryfikowano 22 listopada 2026.

S74: Cyfrowy Polsat, Supplement to the customer-data notice of 29 April 2026. https://www.polsatbox.pl/komunikat-dane-osobowe/. Zweryfikowano 22 listopada 2026.

S75: Energetyka24, Przerwa działania strony podmiotu sektora energii; przytoczone oświadczenie. https://energetyka24.com/ (article URL withheld). Oświadczenie podmiotu przeczytano w artykule; osobny komunikat pierwotny nie był dostępny do weryfikacji. Zweryfikowano 22 listopada 2026.

S76: Public broadcaster, Travel intermediary reports customer-information access. https://www.polskieradio.pl/. Article URL withheld; company statement relayed in reporting, standalone primary notice not located. Zweryfikowano 22 listopada 2026.

S77: Medical provider, Controller notice concerning a software-provider incident. Source URL withheld to protect the organisation. Zweryfikowano 22 listopada 2026.

S78: Teaching hospital, Employee-mailbox access notice. Source URL withheld to protect the organisation. Zweryfikowano 22 listopada 2026.

S79: Hospital, Internal workstation-access privacy notice. Source URL withheld to protect the organisation. Zweryfikowano 22 listopada 2026.

S80: Retail outlet operator, Information about limited file downloading. Source URL withheld to protect the organisation. Zweryfikowano 22 listopada 2026.

S81: Recreation operator, Notice about brief unauthorised camera viewing. Source URL withheld to protect the organisation; document dates govern, rather than its filename. Zweryfikowano 22 listopada 2026.

S82: CERT Polska, Analysis of cifrat Android malware. https://cert.pl/posts/2026/04/analiza-cifrat/. Zweryfikowano 22 listopada 2026.

S83: CBZC, International invoice-fraud enforcement operation. https://cbzc.policja.gov.pl/bzc/aktualnosci/1064,MIEDZYNARODOWA-GRUPA-PRZESTEPCZA-ZATRZYMANA-W-POLSCE.html. Zweryfikowano 22 listopada 2026.

S84: CBZC, Bank and courier phishing enforcement operation. https://cbzc.policja.gov.pl/bzc/aktualnosci/872,Falszywe-linki-prowadzily-do-podstawionych-stron-bankow-policjanci-CBZC-rozbili-.html. Zweryfikowano 22 listopada 2026.

S85: CBZC, Investigation of paid DDoS services. https://cbzc.policja.gov.pl/bzc/aktualnosci/993,Nieletni-oferowali-w-Internecie-uslugi-ataku-DDoS-najmlodszy-mial-12-lat.html. Zweryfikowano 22 listopada 2026.

S86: ThreatFabric, Manic: banking malware and spyware. https://www.threatfabric.com/blogs/manic-blend-between-banking-malware-and-spyware. Zweryfikowano 22 listopada 2026.

S87: Group-IB, RemControl Android banking trojan. https://www.group-ib.com/blog/remcontrol-android-banking-trojan/. Zweryfikowano 22 listopada 2026.

S88: Unit 42, Shadow Campaigns: global espionage research. https://unit42.paloaltonetworks.com/shadow-campaigns-uncovering-global-espionage/. Zweryfikowano 22 listopada 2026.

S89: Firma handlowa, Komunikat dostępu do narzędzia poczty i aktualizacja lutowa. Adres źródła pominięty w celu ochrony organizacji. Zweryfikowano 22 listopada 2026.

Dodatek D. Słownik

Termin	Proste wyjaśnienie
Administrator / procesor	Organizacja ustalająca cel i sposób użycia danych / podmiot przetwarzający na jej polecenie
Bieżąca oferta danych logowania	Ogłoszenie w chwili obserwacji; poprawność konta nadal wymaga sprawdzenia
DDoS	Ruch mający uniemożliwić prawidłowym użytkownikom korzystanie z usługi
DMARC	Żądanie polityki domeny dla poczty bez zgodności uwierzytelniania
SPF / DKIM	Autoryzacja nadawcy i podpisywanie wiadomości używane w uwierzytelnianiu poczty
Rekord delegacji DNSSEC	Rekord strefy nadrzędnej łączący domenę z kluczami; nie dowodzi walidacji całego łańcucha
HSTS	Polityka strony nakazująca przeglądarce połączenia szyfrowane
KSC / S46	Polski krajowy system cyberbezpieczeństwa / system informacji i raportowania
KYC	Sprawdzanie tożsamości przy przyjmowaniu lub weryfikacji klienta
MFA odporne na phishing	Uwierzytelnianie związane z prawidłową usługą, którego zatwierdzenia nie wykorzysta fałszywa strona
Log stealera / combolist	Informacje przechwycone przez malware kradnące dane / zbiór par login i hasło
Toll fraud / direct carrier billing	Nadużycie płatnych usług mobilnych / obciążanie rachunku przez operatora
OT	Systemy monitorowania lub sterowania procesami fizycznymi
TLP:CLEAR	Udostępnianie bez ograniczeń TLP; inne obowiązki nadal obowiązują

O raporcie

Opracowanie Odin by Brandefense. Wersja 1.0, 22 listopada 2026. Angielski tekst główny i polskie wydanie zachowują liczby, identyfikatory dowodów, źródła i dyrektywy. Wersję polską przetłumaczono z pomocą AI; przy rozbieżności rozstrzyga angielska.

Raport jest oceną ograniczoną źródłami, a nie pełnym spisem polskich incydentów. Zalecenia opisują możliwą weryfikację i poprawę. Nie ustalają, że wskazana organizacja nie stosowała zalecanego zabezpieczenia.

© 2026 Brandefense.

ABOUT BRANDEFENSE

Attackers See You First. We make sure you do.

Brandefense is an AI-driven platform that sees your organization the way attackers do, continuously monitoring the open, deep, and dark web to detect phishing campaigns, credential leaks, exposed assets, and threat actor activity before they translate into breaches.

Built for security teams that can no longer afford to wait for threats to arrive at the perimeter, it processes millions of external signals in real time and returns only what demands attention.

Unifying Digital Risk Protection, External Attack Surface Management, and Cyber Threat Intelligence under a single interface, Brandefense gives CISOs and SOC teams the external visibility they have always been missing and the intelligence to act on it with confidence.

GARTNER PEER INSIGHTS
4.7 / 5

COVERAGE
3 pillars
CTI, DRPS, EASM

MONITORING
24 / 7
Open, deep and dark web

REQUEST A DEMO

Request A Demo. See what attackers see.

Discuss your domains, brands and security priorities in a 30-45 minute session with Sales and Presales. A Brandefense team member or a partner in your region will follow up.

Request a demo →

AWARDS

Recognised Around The World. Technology and trust.

Selected awards recognising Brandefense technology and innovation.



Top InfoSec Innovator

2026



Deloitte Technology Fast 500 EMEA

2024



Global InfoSec Awards

2025



Cybersecurity Excellence Awards

2025

See Brandefense In Action.

Bring your domains, brands and security priorities to a 30-45 minute conversation with Sales and Presales.

Request a demo →

BRANDEFENSE

See what attackers see. Before they act.

UNITED STATES

300 Delaware Ave. Ste 210 #328
Wilmington, DE 19801

TÜRKIYE

Üniversiteler Mh., 1605 Cd.
Cyberpark Vakıf Binası No: B25
Çankaya, Ankara

BRANDEFENSE.IO