BRANDEFENSE COUNTRY REPORT · POLAND 2026

Brandefense Poland Cyber Threat Landscape Report 2026

Supplier-held data, identity abuse and recovery decisions across a connected economy

Odin by Brandefense
Research window: 1 January–22 November 2026, by post date
Version 1.0 · Public Research Edition · TLP:CLEAR · 22 November 2026

78 of 250
selected domains had a credential listed for sale when checked

7
selected offer dossiers with distinct claim boundaries

15
detailed official-source case cards, separate from underground offers

56
Polish ransomware listings under 21 group labels

CONTENTS

Contents

01	Executive summary	05
	Report map	09
02	Poland's digital and security context	10
03	National exposure: the selected organisation universe	14
04	What we see on the dark web	24
05	Confirmed incidents and claims by sector	40
06	Hacktivism, DDoS and recent activity	58
07	Threat actors and evidence relationships	64
08	The fraud economy	75
09	Banking and finance deep dive	81
10	Regulatory and national response	86
11	Outlook	90
12	Action plan	94
A	Appendix A. Method and evidence boundaries	101
B	Appendix B. Evidence register	105
C	Appendix C. Sources	106
D	Appendix D. Glossary	110
	About this report	111

Board and CISO	01 05 11 12
SOC and intelligence	04 06 07 12
Identity and infrastructure	03 05 07 12
Finance and fraud	08 09 12
Legal and procurement	05 10 12

About this edition

AI-assisted research and drafting. Observations, criminal claims, official disclosures and analyst interpretations are distinguished throughout. The final observation day is partial.

Poland's verified disclosures make supplier data, account authority and service recovery practical priorities, while underground advertising requires validation before its scale or provenance is accepted.

118,390

country-associated publications [S1]

56

Polish ransomware listings [S3]

78 / 250

selected domains with current credential listings [S2]

22

detailed offer and official-source dossiers

Contents and reading routes

The report moves from decisions to evidence, then to accountable actions. Its twelve chapters preserve the differences between an advertisement, an official incident and an analytical judgement.

Chapter	Question	First reader
1 Executive summary	What should leadership decide first?	Board and CISO
2 Context	Which dependencies make the cases consequential?	Leadership and architecture
3 National exposure	What can the selected-domain observations establish?	Identity and infrastructure
4 Dark-web evidence	What do data and access offers actually claim?	Intelligence and response
5 Sector incidents	Which official accounts change the response?	Service and sector owners
6 DDoS and recent activity	What is claimed, what is confirmed, and what changed recently?	Operations and communications
7 Threat actors	Which attributions and relationships are supported?	Intelligence and SOC
8 Fraud economy	How can accurate information support a false instruction?	Fraud and customer protection
9 Banking	Which financial decisions need joint ownership?	Finance and identity
10 Regulation	Which duties and transition dates apply?	Legal and compliance
11 Outlook	Which signals would change the assessment?	Leadership
12 Action plan	Who acts, and what demonstrates completion?	All owners

Leadership route: Chapters 1, 5 and 10–12. **Operations route:** Chapters 4, 6–7 and 12. **Identity and fraud route:** Chapters 3, 8–9 and 12.

Observed means a post or measurement is retained. **Claimed** means a poster or listing asserts something. **Officially reported** means an organisation or authority disclosed it, within its stated scope.

An analyst interpretation connects evidence to a decision. It does not supply missing proof about access, affected people, state direction, transactions or losses.

CHAPTER 01

Executive summary

01

THIS CHAPTER ANSWERS

Which decisions follow most directly from Poland's verified disclosures and retained evidence?

4

leadership decisions with accountable owners

Four decisions for leaders 07

The year in numbers 07

CHAPTER 01

Executive summary

IN SHORT

Poland's 2026 evidence connects supplier-held information, account abuse and service recovery. Official notices describe healthcare and accounting data incidents, university data publication and staged restoration of public services. Ransompedia records 56 Polish listings; underground offers add claims that need separate validation. The national Atlas headline is 51 out of 100. Prioritise supplier scope, identity verification, independent payment approval and recovery of essential workflows.

1. Shared software can distribute the response across many controllers. The Ministry's MyDr statement identifies a potential scope of 18.8 million people and more than 12,000 facilities, involving historical records. FELG and Fakturownia also distinguish provider investigation from customer-specific assessment. These populations are not added together [S5][S8][S10].

2. Continued service does not resolve a data incident. MyDr's official account reports no interruption to care. The university confirms copying and publication without encryption of key systems. Conversely, ePUAP's November response required staged restoration. Availability, access, copying and misuse require separate answers [S5][S31][S41].

3. Ransomware listings support recovery planning, with a clear visibility limit. Ransompedia holds 56 Poland-labelled listings during the window, under 21 group labels. The Gentlemen accounts for 19. The 32 listings for all of 2025 are a different-duration comparison, not a measured annual growth rate [S3].

4. Recent access advertising is a validation task. A November food-service offer claims a fresh export, while a separate public-body mailbox advertisement claims current inventory. Neither establishes active access, an affected-person total or a connection to the official November incidents. The latter's asking price is a claim about an offer, not a verified sale [S1].

5. Current credential listings make account validation the first exposure task. 78 of 250 selected domains had a credential listed for sale when checked. The national Atlas headline is 51 out of 100. The portfolio contains at least 590,940 device associations and 281,292,486 historical credential-record associations. These overlapping observations do not establish unique people or confirmed intrusions [S2].

Four decisions for leaders

1. **Require supplier-specific scope.** Give procurement and the DPO responsibility for obtaining tenant or practice information after a provider notice. Preserve the awareness decision and assess legal reporting before the final investigation is complete.
1. **Validate account authority.** Give identity operations and the SOC responsibility for checking relevant external offers against active accounts, sessions and prior remediation. Prioritise phishing-resistant authentication for high-impact accounts and test recovery.
1. **Protect sensitive instructions.** Give finance and customer-support owners an independent verification process for payee changes, urgent transfers and notice-themed calls. Test it with accurate synthetic business details.
1. **Prove service recovery.** Give the business owner and infrastructure team a joint restore exercise. Include protected backups, independent administration, data integrity, alternative workflows and a signed acceptance of the actual service.

The year in numbers

The numbers below have different populations and must not be added.

118,390

Country-associated publications in the post-date window [S1]

WHAT IT IS NOT

Attacks, deliberate national targeting or unique offers

119,484

Dis-
tinct retained posts used for this edition [S1]

WHAT IT IS NOT

The complete publication population

56

Ransompedia Poland-labelled listings [S3]

WHAT IT IS NOT

Confirmed encryption events or independently verified unique victims

78 of 250

Selected domains with a credential listed for sale when checked [S2]

WHAT IT IS NOT

Confirmed infrastructure access, valid accounts or a national prevalence estimate

51 / 100

National Atlas headline for the selected portfolio [S2]

WHAT IT IS NOT

A sector rating or an attack probability

182 of 241

DMARC policies requesting quarantine or rejection [S2]

WHAT IT IS NOT

Complete enforcement or phishing prevention

18.8 million

Ministry's potential MyDr population [S5]

WHAT IT IS NOT

A unique-person total independently validated by this report

455

Poland-associated cards visible in clear text in retained posts [S4]

WHAT IT IS NOT

Card theft, valid cards, fraud loss or Brandefense's wider card coverage

22

Seven detailed offer dossiers and fifteen official-notice-led dossiers

WHAT IT IS NOT

A complete national incident count or twenty-two confirmed intrusions

The recent-activity focus is 9–22 November. The final observation day and November are partial. Public disclosures, post dates and intrusion dates remain distinct throughout.

KEY TAKEAWAYS

01

Start with supplier scope, account authority and essential-service recovery.

02

Keep posts, listings, people, files and organisations in separate populations.

03

Escalate on corroborated facts and retain uncertainty where copying or impact remains unresolved.

Report map

Choose the decision you own, then follow its evidence and completion test.

Board and CISO	What deserves funding and management ownership?	01 05 11 12
SOC and intelligence	Which claim requires validation, and which source supports attribution?	04 06 07 12
Identity and infrastructure	Which accounts, configurations and recovery paths need checks?	03 05 07 12
Finance and fraud	What should never authorise an account or payment change?	08 09 12
Legal and procurement	Who controls the data and which clock applies?	05 10 12

Evidence track	Question	Boundary
Retained posts	What is advertised or announced?	Claims need separate validation
Ransomware listings	What is visible in the source snapshot?	Listings are not confirmed incidents
Exposure and passive observations	Which accounts, devices and configurations require validation?	Associations and policy requests are not proof of intrusion
Official disclosures	What does the organisation or authority report?	Estimates and findings can change
Public research	Which campaign behaviours and attributions does a researcher describe?	The source's scope and event dates still apply

CHAPTER 02

Poland's digital and security context

THIS CHAPTER ANSWERS

Which dependencies make the observed incidents consequential for Polish organisations?

90.5%

internet penetration in the October 2026 estimates

2.1 A connected population, with repeated identity touchpoints 11
2.2 Shared software connects independent controllers 11
2.3 Availability and confidentiality require separate answers 11
2.4 Political framing and source attribution 12
2.5 Historical energy reporting informs current planning 12
2.6 Cybersecurity obligations have a specific timetable 12

CHAPTER 02

Poland's digital and security context

IN SHORT

Poland's connected services concentrate identity, health and business information in platforms used by many independent organisations. This year's official notices show supplier data incidents, mobile fraud and prolonged recovery of public services. State-linked assessments need a separate evidence track from criminal advertising. Build the service inventory around identity providers, processors and recovery dependencies, then assign an owner to each.

2.1 A connected population, with repeated identity touchpoints

DataReportal's Digital 2027 Poland edition was published in November 2026. Its October estimates describe 34.2 million internet users, 90.5% penetration, 54.4 million mobile connections and 28.0 million social-media identities. Connections and identities are not unique people [S29].

These figures explain the importance of service dependencies, rather than the probability of an attack. A patient, employee or business owner may use the same contact information across medical, accounting, banking and public-service platforms. A disclosed address can therefore make a later fraudulent message more convincing.

Identity facts should help locate a record. They should not authorise a password reset, bank-account change or disclosure of medical information. This distinction remains useful even when the original data are several years old.

2.2 Shared software connects independent controllers

The MyDr and FELG notices concern software used by independent medical practices. Fakturownia distinguishes information it controls from information customers entrust to it as their processor. A supplier incident can therefore create many separate assessment and notification decisions [S5][S8][S10].

A procurement list alone cannot reveal this dependency. An effective register identifies the application, data categories, controller, processor, subcontractors, administrator accounts and business process. It also records who can obtain an account-specific incident assessment when a provider publishes a general notice.

This does not establish that every customer of an affected supplier lost data. The relevant unit changes between a platform, a customer account, a practice, a record and a person. The report keeps those units separate.

2.3 Availability and confidentiality require separate answers

The Ministry's MyDr notice said the incident did not interrupt ongoing care, including prescription issuance. The public document platform ePUAP required staged restoration after its November incident. These accounts demonstrate different service consequences [S5][S31].

A service can continue operating while historical information has been accessed. A precautionary restriction can also last after an immediate threat has been contained. Neither situation, by itself, determines whether personal data were copied.

Business owners should prepare two assessments: which work can continue, and which information may have been disclosed. Communications should publish each answer with its own evidence and update time.

2.4 Political framing and source attribution

CERT Polska names UNC1151/Ghostwriter in its June phishing report. Its January energy report compares infrastructure with a named activity cluster. ZeroFox describes politically framed DDoS claims involving Poland. These are the sources' assessments within their respective scopes [S14][S18][S30].

Russian-language advertising does not establish a Russian operator, state direction or a link to an intelligence service. The same applies to Belarusian references, Ukrainian themes, patriotic slogans and claims about elections. Language, claimed motive, technical association and state attribution answer different questions.

The report takes no position on government decisions, international relations or political disputes. It does not infer that a domestic policy caused an incident. A source's attribution is introduced as that source's attribution, rather than as an independently established conclusion.

2.5 Historical energy reporting informs current planning

CERT Polska's January report concerns attacks on 29 December 2025. It describes at least 30 renewable-energy sites, a manufacturing business and a combined heat and power plant. The report says electricity production and end-user heat supply were not interrupted as the attacker intended [S18].

These events precede the report's incident window. Their January publication and later supplementary reporting are relevant 2026 disclosures, but do not turn them into new 2026 attacks. They are not added to this year's case count.

The useful question for operators is whether recovery covers field devices, remote management and communications as well as servers. A restored office network does not demonstrate that an industrial process can be controlled safely.

2.6 Cybersecurity obligations have a specific timetable

Poland's KSC amendment entered into force on 3 April 2026. The Ministry subsequently published registration, implementation and audit milestones. Its detailed guidance distinguishes new essential entities from existing operators with an ongoing audit cycle [S25][S26].

At the cut-off, the initial 3 October registration milestone was already past for entities meeting the specified conditions. The 3 April 2027 implementation milestone was still ahead. Legal teams should determine the entity's status and applicable transition provisions, rather than treating all dates as universal extensions.

KEY TAKEAWAYS

01

Map processors and identity recovery alongside applications and servers.

02

Separate continued service from evidence about data confidentiality.

03

Keep historical events and source-attributed state assessments distinct from this year's incident population.

CHAPTER 03

National exposure: the selected organisation universe

03

THIS CHAPTER ANSWERS

What exposure is associated with the selected domains, and which validation should come first?

78 of 250

selected domains had a credential listed for sale when checked

3.1 Universe card 15
3.2 National Atlas headline and sector observations 16
3.3 Devices and historical credential records 17
3.4 Current listings create an account-validation task 19
3.5 Documents, lookalikes and mentions 19
3.6 Email-authentication observations 20
3.7 DNS, TLS and web observations 22
3.8 Validation before prioritisation 22

CHAPTER 03

National exposure: the selected organisation universe

IN SHORT

78 of 250 selected domains had a credential listed for sale when checked. The national Atlas headline is 51 out of 100. The portfolio contains at least 590,940 device associations and 281,292,486 historical credential-record associations. These observations overlap and do not establish unique people or confirmed intrusions. Validate current accounts and sessions first, then investigate employee devices and review email authentication.

3.1 Universe card

The selected list represents candidate organisation associations. Legal ownership, organisational independence and alias completeness require further validation. The results describe this portfolio, rather than national prevalence or a validated organisation ranking [S2].

Item	Definition
Selected universe	250 candidate domains spanning twelve public and private sectors; one primary domain per candidate organisation
Selection	Purposive, based on institutional role and sector prominence; not an official revenue ranking
Passive population	241 domains with passive observations; 9 candidates without those observations
Exposure population	250 domains with exposure observations; a source association does not establish current legal ownership
Dates	Exposure counts read 21 November 2026; additional source counts and passive checks read 22 November 2026
Periods	Device, credential, document and listing observations describe records held when checked, including older material. Mentions cover the preceding 365 days to 22 November; lookalikes cover 30 days to 21 November
Overlap	Associations are not unique people or devices across sources or organisations; the same account or device can concern several domains
Inference limit	No national prevalence, verified-intrusion total or control-effectiveness estimate

3.2 National Atlas headline and sector observations

78 of 250 selected domains had a credential listed for sale when checked [S2].

The national Atlas headline for the selected portfolio is 51 on a scale from 0 to 100. Higher values mean greater observed exposure. The report publishes this national figure only. The sector table contains observed signal counts, with no sector or organisation ratings [S2].

51 / 100

national Atlas headline for the selected portfolio

78 / 250

selected domains with a current credential listing

246 / 250

selected domains with historical credential records

The heatmap compares the presence of separate signals. A current listing means a credential associated with the domain was offered when checked; listing history refers to earlier offers. Neither establishes account validity or a completed sale.

Current listings and employee-device associations vary across the selected sectors

Selected domains with each signal, shown over the sector denominator. Current credential listings are shown in coral.

	Infected devices	Employee devices	Credential records	Current listing	Listing history	Lookalikes (30 days)	Exposed documents
Banking and finance	29/30	21/30	30/30	10/30	10/30	28/30	15/30
Education	30/30	29/30	30/30	14/30	13/30	29/30	24/30
Energy and utilities	20/20	17/20	19/20	5/20	4/20	16/20	8/20
Government	49/50	38/50	49/50	7/50	7/50	47/50	36/50
Healthcare	10/10	7/10	10/10	4/10	4/10	10/10	4/10
Hospitality and tourism	8/10	6/10	10/10	4/10	4/10	9/10	5/10
Insurance	10/10	8/10	10/10	4/10	4/10	9/10	6/10
Manufacturing and industry	25/30	22/30	29/30	2/30	2/30	17/30	10/30
Media and entertainment	10/10	7/10	10/10	4/10	4/10	10/10	9/10
Retail and holdings	18/20	18/20	19/20	15/20	15/20	18/20	15/20
Telecom and technology	10/10	9/10	10/10	4/10	4/10	10/10	6/10
Transport and logistics	20/20	14/20	20/20	5/20	5/20	15/20	8/20

Source: Brandefense exposure observations for 250 selected candidate domains, read 21 November 2026. Cumulative associations can overlap and do not establish unique people or confirmed intrusions [S2].

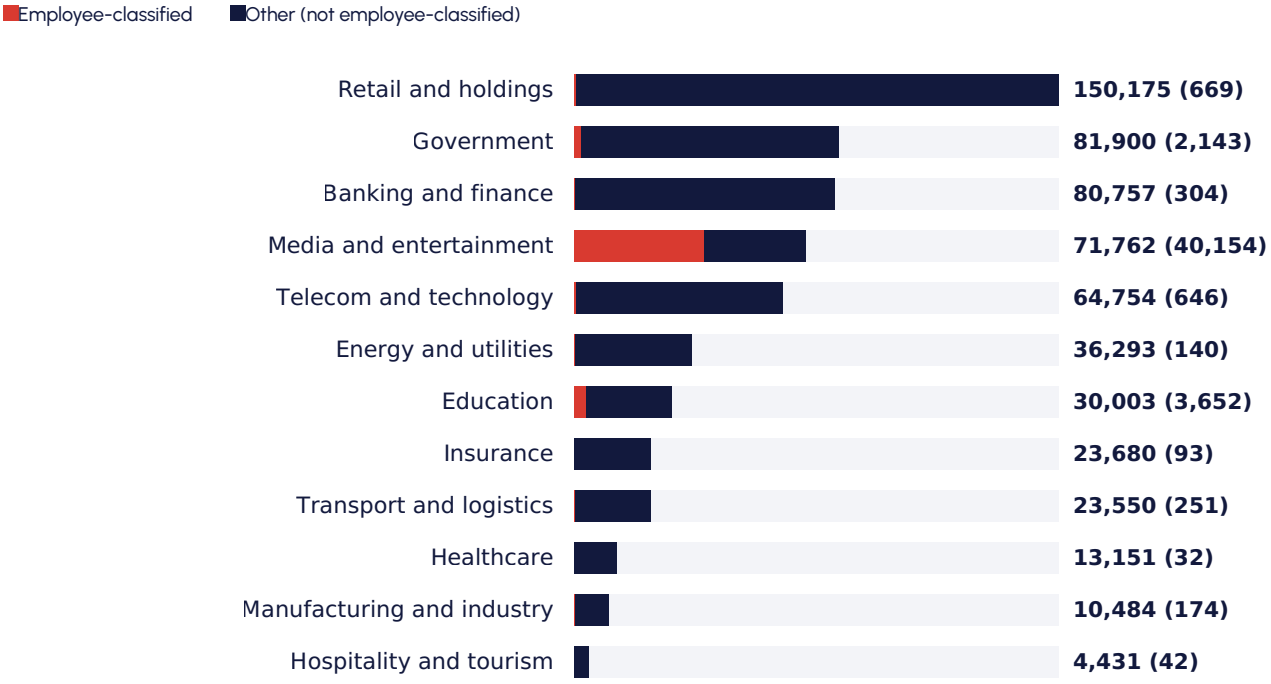
All signal columns count candidate domains. In the H01 and C04 downloads, `candidate_domains` is the selected-domain count for each sector. H01's `candidate_domains_with_listing_history` counts domains with earlier offers, rather than individual offers.

Sector	Domains	Domains with current listings	Domains with listing history	Domains with employee-device associations	Domains with document references
Government	50	7	7	38	36
Banking and finance	30	10	10	21	15
Education	30	14	13	29	24
Manufacturing and industry	30	2	2	22	10
Energy and utilities	20	5	4	17	8
Retail and holdings	20	15	15	18	15
Transport and logistics	20	5	5	14	8
Telecom and technology	10	4	4	9	6
Healthcare	10	4	4	7	4
Insurance	10	4	4	8	6
Hospitality and tourism	10	4	4	6	5
Media and entertainment	10	4	4	7	9
All selected	250	78	76	196	146

3.3 Devices and historical credential records

C04 separates employee-classified device associations from other device associations. Ownership of the other devices is not established; customers, students, contractors and older accounts are possible explanations [S2].

Device associations span customer-facing sectors, public bodies and education



Source: Brandefense exposure observations for 250 selected candidate domains, read 21 November 2026. Cumulative associations can overlap and do not establish unique people or confirmed intrusions [S2].

Sector	Domains with devices	Device associations	Employee associations	Credential records
Retail and holdings	18 / 20	150,175	669	57,439
Government	49 / 50	81,900	2,143	273,278
Banking and finance	29 / 30	80,757	304	54,584
Media and entertainment	10 / 10	71,762	40,154	271,636,420
Telecom and technology	10 / 10	64,754	646	8,537,438
Energy and utilities	20 / 20	36,293	140	26,862
Education	30 / 30	30,003	3,652	596,069
Insurance	10 / 10	23,680	93	28,064
Transport and logistics	20 / 20	23,550	251	29,373
Healthcare	10 / 10	13,151	32	10,971
Manufacturing and industry	25 / 30	10,484	174	30,899

Sector	Domains with devices	Device associations	Employee associations	Credential records
Hospitality and tourism	8 / 10	4,431	42	11,089
All selected	239 / 250	590,940	48,300	281,292,486

Some device totals are lower bounds. Employee associations are included within the device total and must not be added to it. Historical credential records can repeat accounts, people and older captures; they do not identify active credentials.

The credential population comprises 89,719,574 breach-database records, 15,418,280 stealer-log records and 176,154,632 combolist entries. These source associations are not a count of Polish residents. The large media and entertainment total should be validated within its source and account scope.

≥590,940

device associations, including employee-classified devices

48,300

employee-classified device associations

281,292,486

historical credential-record associations

3.4 Current listings create an account-validation task

78 of 250 selected domains had a credential listed for sale at the snapshot. A listed account can belong to a customer, employee or another user. The listing does not establish that the organisation's infrastructure was accessed [S2].

Identity operations should check whether the relevant account is active, whether prior remediation covered it, and whether sessions or recovery changes are suspicious. Validate ownership and freshness before revoking access or imposing a disruptive password reset.

3.5 Documents, lookalikes and mentions

The table describes references and resemblance candidates, rather than confirmed sensitive-document exposure or malicious domains. An associated document may be public, obsolete or unrelated to an active organisational system. A similar name needs owner validation [S2].

Sector	Documents	Lookalike candidates	Domains with lookalikes
Government	8,253	10,818	47
Banking and finance	56	4,883	28

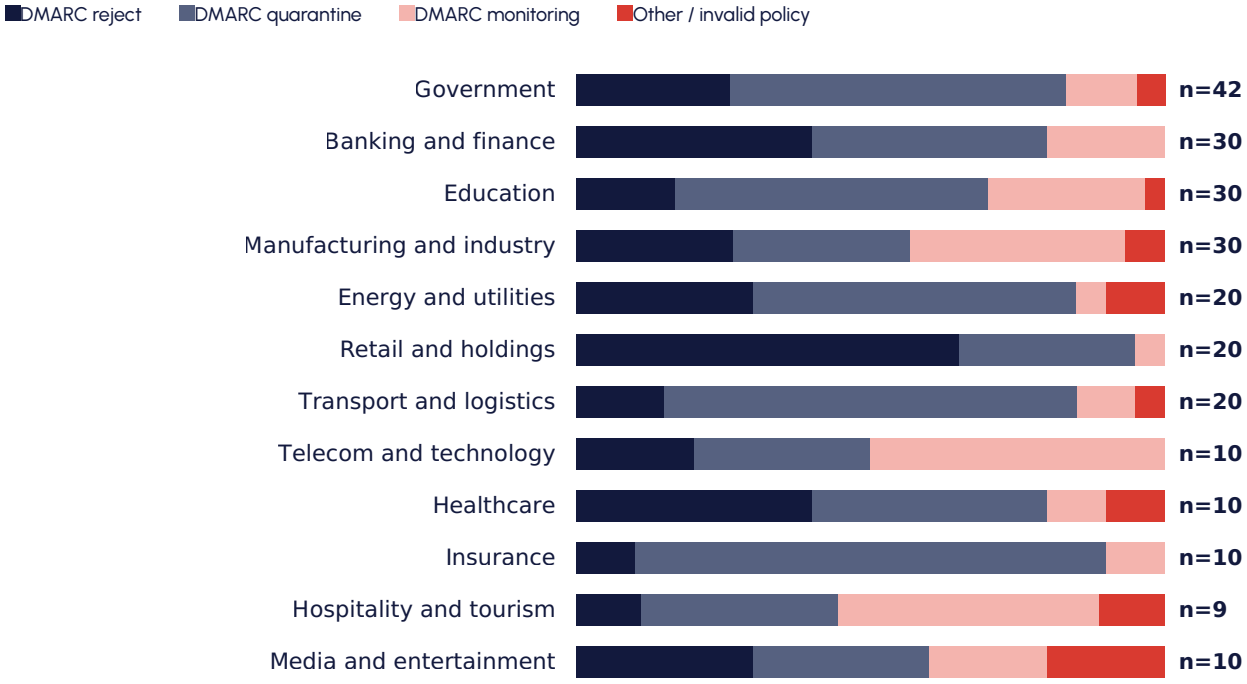
Sector	Documents	Lookalike candidates	Domains with lookalikes
Education	133	25,129	29
Manufacturing and industry	25	1,066	17
Energy and utilities	10	6,036	16
Retail and holdings	91	7,506	18
Transport and logistics	61	16,608	15
Telecom and technology	66	21,542	10
Healthcare	4	798	10
Insurance	12	555	9
Hospitality and tourism	66	2,641	9
Media and entertainment	1,333	996	10
All selected	10,110	98,578	218

The selected domains have 2,518 chat-source mentions and 998 web-source mentions during the preceding 365 days. Mentions can include commentary, advertising and repeated references. They do not measure distinct actors, attacks or verified access.

3.6 Email-authentication observations

Passive observations have their own denominator. The chart records requested mail policy, without measuring acceptance, spoofing success or implementation across every legitimate sender.

DMARC policy requests vary across the selected sectors



Source: public passive observations for 241 selected domains, read 22 November 2026. Each sector uses its observed-domain denominator; policy requests do not establish enforcement [S2].

Sector	Domains	Quarantine or reject	Monitoring	Other or unobserved
Government	42	35	5	2
Banking and finance	30	24	6	0
Education	30	21	8	1
Manufacturing and industry	30	17	11	2
Energy and utilities	20	17	1	2
Retail and holdings	20	19	1	0
Transport and logistics	20	17	2	1
Telecom and technology	10	5	5	0
Healthcare	10	8	1	1
Insurance	10	9	1	0
Hospitality and tourism	9	4	4	1

Sector	Domains	Quarantine or reject	Monitoring	Other or unobserved
Media and entertainment	10	6	2	2
All observed	241	182	47	12

The 182 quarantine or rejection requests represent 75.5% of 241 observed domains. They comprise 69 rejection and 113 quarantine policies. This does not establish complete rollout, alignment or enforcement by recipients [S2].

SPF records were observed for 237 domains and DKIM signing records for 154. Absence from an observation is not proof that a domain never signs mail. Compare actual senders and authentication results before changing delivery behaviour.

3.7 DNS, TLS and web observations

Inconclusive observations are neither successful validation nor confirmed control failures. Each row keeps its own denominator [S2].

Observation	Result	Interpretation boundary
DNSSEC delegation record	20 of 241	A delegation record alone does not establish validation of the whole chain
Conclusive TLS validation	234 of 241	7 results were inconclusive
Successful TLS validation	227 of 234	The observed connection, not every service or client
TLS validation failures	7 of 234	Require owner validation; no evidence of unauthorised access
Homepage responses	196 of 241	A response is not an ownership or application-security assessment
HSTS observed	129 of 196	Responding homepages only; not every subdomain or user

3.8 Validation before prioritisation

Identity operations should match an external signal to an active account and its sessions. Employee-device investigation and customer-account protection require separate owners. Historical records alone should not trigger a claim of current intrusion.

Messaging owners should identify legitimate senders and examine authentication alignment before tightening policy. Completion requires legitimate delivery and rejection of unauthorised use in an approved test. Publishing a record alone does not demonstrate that outcome.

Infrastructure owners should investigate validation failures and inconclusive observations against their own service configuration. Redirects, legacy domains and organisational boundaries can change the appropriate inventory. No causal link between a configuration observation and an incident is inferred.

KEY TAKEAWAYS

01

Validate current listings against active accounts and session evidence.

02

Keep employee devices, other devices and historical credential records within their own scopes.

03

Use the national Atlas headline alongside measured signals and verified ownership.

CHAPTER 04

What we see on the dark web

04

THIS CHAPTER ANSWERS

What do Polish data and access advertisements establish, and what still needs validation?

7 selected offer dossiers with distinct claim boundaries

4.1 Universe card 25
4.2 Volume, platforms and language 25
4.3 Illustrative crime-family observations 27
4.4 Poland-specific offers 28
4.5 Case A: a public-service access offer (B01) 29
4.6 Case B: a patient-account extract claim (B02) 30
4.7 Case C: a recent food-service dataset offer (B03) 31
4.8 Case D: a travel offer with an uncertain country denominator (B04) 32
4.9 Case E: users and database lines are different quantities (B05) 33
4.10 Case F: repeated retailer promotion (B06) 34
4.11 What the retained evidence does not connect 35
4.12 Additional offers and government-themed services 35
4.13 Case U: telecom files and helpdesk access (B12) 37
4.14 Smaller datasets and privileged-access advertising 38

CHAPTER 04

What we see on the dark web

IN SHORT

Poland-associated posts advertise access, customer records, identity material and accounts. Seven selected forum dossiers show why quantity, freshness and provenance must remain separate claims. A travel offer's records are not necessarily Polish residents, a food-order database's lines are not people, and patient-account credentials do not establish a provider intrusion. Validate each relevant offer against your own account and data evidence before escalating its claimed scale.

4.1 Universe card

The publication counts and retained content describe different populations. The country association does not itself establish deliberate targeting of Poland [S1].

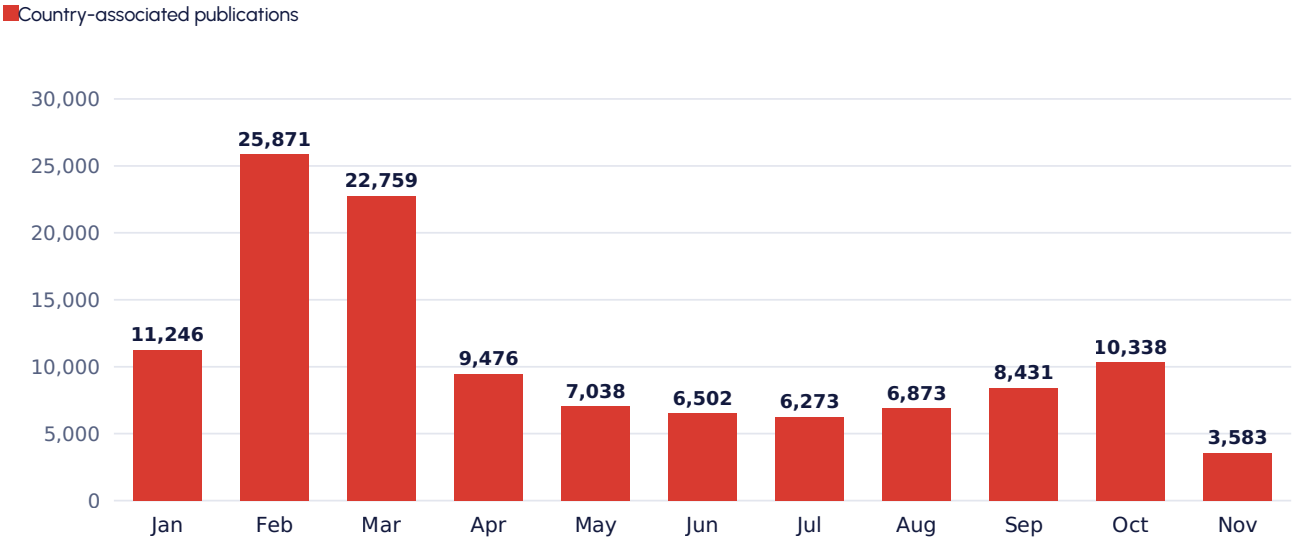
Item	Population or boundary
Window	1 January–22 November 2026, by post date; the final day is partial
Country-associated publication count	118,390 tagged posts; advertisements, commentary and repeated material are included
Retained content	119,484 distinct posts across the retained country and related material
Retained platforms	1,434 forum, 117,911 Telegram, 69 paste, 70 Discord
Recent retained population	2,123 posts dated 9–22 November; not a national incident count
Selected cases	Seven offer dossiers, A–F and U, supported by B01–B06 and B12
Not established	Authenticity of an offered file, active access, unique people, a completed sale or national incident prevalence

Retained country-associated content contains 118,387 posts within the publication population of 118,390. Related-source coverage remains partial. The report does not extrapolate retained-post category counts into national crime totals.

4.2 Volume, platforms and language

The monthly chart shows the publication population, rather than the volume of newly occurring incidents. February contains 25,871 posts and March 22,759. November contains 3,583 at the snapshot and is incomplete [S1].

Country-associated publication volume is not a national incident trend



Source: Brandefense retained Poland publications, 1 January-22 November 2026; November partial. Language labels can overlap; publications are not incident counts [S1].

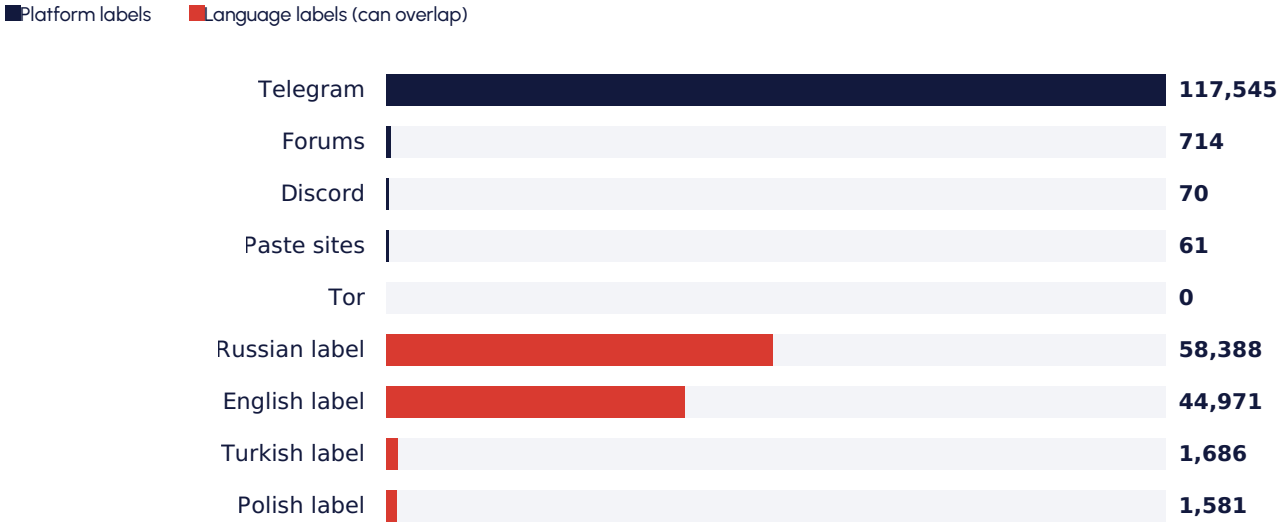
Changes can reflect advertising, source visibility and collection coverage. The chart does not demonstrate that attacks peaked in February or that a later decline represents improved security. Posts may refer to older information or list several countries together.

The retained platforms are dominated by Telegram and forums. That describes the retained material, not the relative importance of every criminal venue. Closed exchanges, deleted content and private transactions are outside this evidence.

English, Russian, Polish and Turkish appear in the retained material. Source language labels can overlap and include inconsistent results. This edition therefore does not publish a language-based estimate of criminal nationality or a national language-market ranking.

The publication population has the platform and language observations below. Language labels can overlap; their counts must not be added. These are publication labels, not criminal nationality or unique actor counts [S1].

Platform and language labels describe publications, rather than verified attackers



Source: Brandefense retained Poland publications, 1 January–22 November 2026; November partial. Language labels can overlap; publications are not incident counts [S1].

Dimension	Label	Publications
Platform	Telegram	117,545
Platform	Forums	714
Platform	Discord	70
Platform	Paste sites	61
Platform	Tor	0
Language label	English label	44,971
Language label	Polish label	1,581
Language label	Russian label	58,388
Language label	Turkish label	1,686

4.3 Illustrative crime-family observations

A descriptive content assessment identifies 43,320 potentially relevant posts within 118,387 retained country-associated posts. Categories overlap. The table describes this content population, without estimating national crime prevalence [S1].

Activity family	Posts	What it suggests	What it does not establish
Financial-account trading	15,496	Accounts and payment access are advertised	Completed trades or cash-out value

Activity family	Posts	What it suggests	What it does not establish
Data and database offers	12,028	Identity and business records have advertising value	Newly affected people or the original source
Identity documents and verification material	9,458	Identity-check processes are of interest	Genuine documents or successful verification
Phishing and fraud material	5,944	Services and tools are promoted	Their deployment against a Polish organisation
Card-related material	6,179	Payment-card themes appear in posts	Distinct cards or fraud loss
Initial-access offers	823	Access is advertised as a product	Current control over the claimed organisation
Login combinations	1,245	Credential collections are distributed	Account validity or capture method

Counts must not be added across rows. A single post can advertise several products. Card-themed posts are also a different population from the distinct cards in Chapter 8.

4.4 Poland-specific offers

The selected dossiers preserve the units used by the advertisers. None of these seven claims is treated as an officially confirmed incident.

Card	Posted	Generic target	Advertised unit	Status
B01	2026-02-27	Public-service organisation	Access; more than ten hosted domains; USD 200	Access and ownership unverified
B02	2026-08-21	Healthcare service	116 credential records	Validity, access and medical-data exposure unverified
B03	2026-11-15	Consumer food service	A claimed 72K dataset	Size unit and freshness unverified
B04	2026-05-11	Travel intermediary	A claimed 10.3 million records	Polish-resident denominator and provenance unverified
B05	2026-01-05	Consumer ordering platform	239,434 users and 7,456,341 lines claimed	Separate units, both unverified

Card	Posted	Generic target	Advertised unit	Status
B06	2026-02-02	Online retailer	A claimed 100K lines	Unique customers and acquisition date un-verified
B12	2026-03-20	Telecommunications service	About 29,578 files; 17,556 user rows; 51,936 ticket rows claimed	Units, authenticity and current helpdesk ac-cess unverified

4.5 Case A: a public-service access offer (B01)

Evidence card B01 27 Feb 2026

metadata Forum Forum English

ORIGINAL

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

Held

The offer claims server access, documents and database material, with more than ten hosted domains.

Not established

Current access, ownership, document sensitivity and copying are unverified.

A

CASE A

A public-service access offer

Evidence card B01 | 27 Feb 2026 | Forum | Public administration

Unverified advertisement

CLAIM	A 27 February forum advertisement offered server access associated with a public-service organisation. It claimed more than ten hosted domains, databases and documents, with an asking price of USD 200.
WHAT IS HELD	The retained post includes an access narrative and operating-system output. Those artifacts support the existence and content of the advertisement. They are not an independently reproduced access test.
WHAT REMAINS UNVERIFIED	Current access, ownership, the nature of the documents and any copying are unresolved. A hosted-domain count is not a count of affected organisations. The report does not open the advertised document link or test the offered account.
ALTERNATIVES	

Shared hosting, recycled access, an unrelated customer environment or fabricated output could fit the advertisement. The post's government association needs validation at the asset and account level.

RESPONSE

Public-service owners should inventory hosting and administrative access, including contractors. Match any relevant external signal to an owned asset and active account before disruptive action. Preserve the reason for the final disposition.

Bottom line

Current access, ownership, document sensitivity and copying are unverified.

4.6 Case B: a patient-account extract claim (B02)

Evidence card B02 21 Aug 2026

updap | Forum | Forum | English

ORIGINAL

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

Held

The post claims 116 patient-account credential records and no MFA.

Not established

Validity, unique people, medical-data access and the provider control claim are unverified.

B

CASE B

A patient-account extract claim

Evidence card B02 | 21 Aug 2026 | Forum | Healthcare

Unverified advertisement

CLAIM

The 21 August post advertised 116 patient-account credential records. It claimed access to medical information and absence of MFA. Those are the poster's assertions, including the control claim.

WHAT IS HELD

The post describes a login-collection format and a points-based access restriction. The existence of that format does not establish where credentials originated. No advertised records were acquired or tested for this report.

ALTERNATIVES

Reused passwords, endpoint-derived credentials, inactive accounts or fabricated entries could fit the description without a provider-system intrusion. Neither the record count nor the advertised medical scope is independently established.

RESPONSE	The provider's identity team should validate relevant accounts and sessions through an authorised process. Privacy staff should investigate medical-data access only where evidence supports it. The report does not infer that the provider lacked MFA from the advertisement.

Bottom line

Validity, unique people, medical-data access and the provider control claim are unverified.

4.7 Case C: a recent food-service dataset offer (B03)

Evidence card B03 15 Nov 2026

Sophia | Forum | Forum | English

ORIGINAL

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

Held

The advertisement claims a 72K dataset and a 15 November export. Visible headings describe orders and contacts.

Not established

Authenticity, freshness, unique people and payment-card exposure are unverified.

CASE C

C

A recent food-service dataset offer

Evidence card B03 | 15 Nov 2026 | Forum | Consumer services

Unverified advertisement

CLAIM	A 15 November advertisement offered a food-service dataset labelled 72K and claimed an export on the same date. Displayed table headings concerned contacts, delivery addresses, orders, instructions and payment status.
WHAT IS HELD	The advertisement and its described structure are retained. The date is a claimed export date. It is not a verified access, extraction or intrusion time.
ALTERNATIVES	A historical order database, reseller material, fabricated sample or several rows per customer could fit the visible description. The 72K label has no established unique-person denominator.
RESPONSE	A relevant service should compare the claimed structure with current and legacy systems and suppliers. Customer support should prepare for calls quoting genuine delivery details. A payment-status field does not establish exposure of payment-card information.

Bottom line

Authenticity, freshness, unique people and payment-card exposure are unverified.

4.8 Case D: a travel offer with an uncertain country denominator (B04)

Evidence card B04 — 11 May 2026

MDGhost | Forum | Forum | English

ORIGINAL

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

Held

The advertisement claims 10.3 million travel records associated with an intermediary with a Poland connection.

Not established

Authenticity, access, acquisition date and the number of Polish residents are unverified.

CASE D

D

A travel offer with an uncertain country denominator

Evidence card B04 | 11 May 2026 | Forum | Travel services

Unverified advertisement

CLAIM	The 11 May post advertised 10.3 million travel records, with identity and contact fields. Related thread titles also referred to dashboard access. The retained body does not validate that access.
WHAT IS HELD	A substantive advertisement links the claimed dataset to a travel intermediary with a Poland connection. Similar wording appears elsewhere in the retained material. That supports advertising continuity, rather than file identity or an independently confirmed repeated incident.
ALTERNATIVES	A multinational booking collection, third-party data or older material could be advertised under the intermediary's name. The displayed geography is not limited to Poland. The record total cannot become a count of Polish residents.
COUNTERCLAIM	A later reply disputes authenticity and describes the offer as a repost of allegedly fake March material. That reply is adverse evidence, rather than an independent file assessment. The report resolves neither claim by accepting the other [S1].

RESPONSE

Travel businesses should examine booking suppliers and customer-notification dependencies. A credible travel-themed message should still require independent validation before a refund, account change or new payment instruction is accepted.

Bottom line

Authenticity, access, acquisition date and the number of Polish residents are unverified.

4.9 Case E: users and database lines are different quantities (B05)

Evidence card B05 — 5 Jan 2026

daghetiaw | Forum | Forum | English

ORIGINAL

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

Held

The post claims 239,434 users and 7,456,341 lines. These are different units.

Not established

Authenticity, claimed date, unique people and exposure of all listed fields are unverified.

CASE E

E

Users and database lines are different quantities

Evidence card B05 | 5 Jan 2026 | Forum | Consumer services

Unverified advertisement

CLAIM	A 5 January post advertised 239,434 registered users and 7,456,341 database lines at a consumer ordering platform. It supplied a dump date in its own date format and described identity, contact, delivery and operational fields.
WHAT IS HELD	The substantive narrative and schema-like material are retained. The report does not reproduce personal values or treat the listed fields as proven exposure. Replies and mirrors add visibility, without validating the original assertion.
ALTERNATIVES	Database lines can include repeated orders, technical tables and configuration. A historical backup, relabelled collection or fabricated extract could produce the advertisement. No ratio between users and lines establishes a meaningful affected-person estimate.

RESPONSE	A service should compare structure and relevant dates through its authorised incident process. Separate user accounts, customer identities and transactional rows when assessing impact. Public communication should preserve those units.

Bottom line

Authenticity, claimed date, unique people and exposure of all listed fields are unverified.

4.10 Case F: repeated retailer promotion (B06)

Evidence card B06 — 2 Feb 2026

Robert2025 | Forum | Forum | English

ORIGINAL

Country: Poland lines: 100K

Held

The advertisement claims 100K retailer lines. Later posts promote the thread.

Not established

Authenticity, freshness, unique customers and a completed transaction are unverified.

CASE F

F

Repeated retailer promotion

Evidence card B06 | 2 Feb 2026 | Forum | Retail

Unverified advertisement

CLAIM	A 2 February post offered a Polish retailer dataset labelled 100K lines. Later retained activity mostly promotes the same advertising thread. Repetition is not independent corroboration.
WHAT REMAINS UNVERIFIED	The report does not establish authenticity, unique customers, capture date or current access. An advertised middleman or transaction arrangement does not validate the data.
ALTERNATIVES	An old backup, duplicated order records, reseller bundle or fabricated material could fit the offer. The advertisement does not resolve those possibilities.
RESPONSE	Retailers should review relevant customer exports, suppliers and access logs when a matching signal appears. Record whether an apparent match concerns old material already handled. Avoid presenting every promotional reply as a new incident.

Bottom line

Authenticity, freshness, unique customers and a completed transaction are unverified.

4.11 What the retained evidence does not connect

The retained offer corpus does not establish a link between these dossiers and the officially disclosed MyDr, Medyc, FELG, Fakturownia or Autopay cases. Similar sector themes are insufficient to join them. The fifteen official-notice-led case cards in Chapter 5 remain a separate track.

The recent food-service offer is a current advertisement, with unverified freshness. A forum item repeating the ePUAP story is news, rather than an additional source proving the incident. The Ministry's own account supplies that corroboration [S31].

4.12 Additional offers and government-themed services

A 16 November service advertisement lists a public-body mailbox for USD 550 and claims current inventory. It does not supply proof of mailbox control in the retained text. Fabricated inventory, resale or an impersonation service remain alternatives (B08).

An August postal-data offer describes sender and recipient fields without an established total or source. A merchant integration could hold similar data. A November shipment offer contains Poland-labelled examples, without establishing a Polish-only population or a breach of a Polish organisation (B09, B11).

A 27 April marketplace offer claims 23 million records and asks USD 1,980. Minimal contact fields could reflect public listings, aggregated leads, recycled information or fabrication. Neither the scale nor a platform intrusion is established (B10).

Evidence card B08 16 Nov 2026

kenpiraa Forum Forum English

ORIGINAL

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

Note. Omission marked; advertised inventory and price remain claims.

Held
The advert prices a purported public-body mailbox at USD 550 and claims current inventory.

Not established
Inventory, mailbox control, access and successful requests are unverified.

Evidence card B09 23 Aug 2026

updap Forum Forum English

ORIGINAL

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

Held
The post claims sender and recipient data and displays a field structure.

Not established
Authenticity, record count, freshness and intrusion into the postal operator are unverified.

Evidence card B10 27 Apr 2026

xcgtyrewty Forum Forum English

ORIGINAL

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

Held
The advertisement claims 23 million records and asks USD 1,980.

Not established
Authenticity, unique people, provenance, date and a platform intrusion are unverified.

Evidence card B11 13 Nov 2026

thisversace Forum Forum English

ORIGINAL

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

Held
The post displays shipment headers and Poland-labelled examples.

Not established
Authenticity, freshness, unique recipients, a Polish-only population and file provenance are unverified.

These are supplementary advertising observations. They are not added to the seven detailed offer dossiers or to official incident counts.

4.13 Case U: telecom files and helpdesk access (B12)

Evidence card B12 — 20 Mar 2026

Katarinka | Forum | Forum | English

ORIGINAL

POLISH ISP DATABASE+FILES+HELPDESK ACCESS

Held

The advert claims telecom files, user rows, support tickets and helpdesk access.

Not established

Authenticity, freshness, unique subscribers and working access are unverified.

CASE U

U

Telecom files and helpdesk access

Evidence card B12 | 20 Mar 2026 | Forum | Telecommunications

Unverified database and access advertisement

CLAIM	A 20 March advertisement offers a Polish telecom database, files and help-desk access. It claims about 29,578 files, a 17,556-row user export and 51,936 ticket rows. Those units are not interchangeable [S1].
WHAT IS HELD	The narrative lists database exports, support-system roles and attachment categories. Its headings include contracts, invoices, installation information and identity-document fields. These establish what the poster advertised, without validating the underlying files or accounts.
WHAT REMAINS UNVERIFIED	Authenticity, current helpdesk access, the acquisition date and unique sub-scribers are unestablished. The described main file categories do not provide a complete reconciliation of the headline. Ticket rows can repeat a subscriber or concern internal work.
ALTERNATIVES	An older service export, contractor copy, mixed collection or fabricated inventory could fit the narrative. A claimed administrative role does not independently establish possession of a working session.
RESPONSE	Telecom operators should review support exports and attachment repositor-ies together with remote administration. Match a relevant signal to an owned system and data structure. Validate access, privileges and the specific data scope through an authorised process.

Bottom line

Authenticity, freshness, unique subscribers and working access are unverified.

4.14 Smaller datasets and privileged-access advertising

An April website-database advertisement claims four application tables with 489 rows, including six user-table rows. Its 9,338-row grand total also includes system-schema metadata. That larger total should not become a customer count; credential validity and administrative privilege remain unverified (B13) [S1].

One 6 April broker post contains two anonymous Polish VPN offers, associated with construction and education. It advertises different privileged roles. Neither current access nor the claimed privilege is established, and a shared advertisement does not prove common ownership of the environments (B14) [S1].

Evidence card B13 6 Apr 2026

Katarinka Forum Forum English

ORIGINAL

Application Tables: 4 Application Rows Total: 489

Held
The advert claims four application tables with 489 rows, including six user rows.

Not established
Authenticity, credential validity and privileges are unverified; the larger total includes metadata.

Evidence card B14 6 Apr 2026

KazeFreak Forum Forum English

ORIGINAL

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

Held
One post advertises two anonymous Polish VPN offers with different claimed roles.

Not established
Current access, privileges and any relationship between the environments are unverified.

Other retained offers illustrate the date and provenance limits. A March retail advertisement explicitly labels its alleged leak as 2025. A large credential compilation admits repeated email addresses with different passwords. Neither a current posting date nor a large line total establishes a new organisational intrusion [S1].

An April vulnerability-sale advertisement names anonymous Polish commercial targets. It is a seller's capability claim, without established exploitation, current control or impact. Treat it as an asset-validation lead, rather than evidence of a completed incident [S1].

A 16 May commercial-website dump post claims credential and name fields in text attachments, without a row total or acquisition date. It allows that passwords may be hashed. The attachment contents, validity and current website access are not established (B15) [S1].

Evidence card B15 — 16 May 2026

org1877 | Forum | Forum | English

ORIGINAL

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

Held

The post claims a commercial-website dump and three text attachments with credential and name fields.

Not established

Authenticity, attachment content, password format, unique people and current access are unverified.

KEY TAKEAWAYS

01

Keep advertised access, data quantities and freshness as separate claims.

02

Similar posts establish advertising continuity, not file identity or common ownership.

03

Validate relevant accounts and data structures before adopting a claimed affected-person total.

CHAPTER 05

Confirmed incidents and claims by sector

THIS CHAPTER ANSWERS

Which disclosures change the response for each sector, and which uncertainties remain?

5.1 Sector decisions 41
5.2 Case G: MyDr and historical medical records 42
5.3 Case H: Medyc and the boundary between investigation and scale 43
5.4 Case I: KELG and provider claims about identity 44
5.5 Case J: Fakturownia and downstream payment fraud 45
5.6 Case K: the University of Warsaw's changing assessment 46
5.7 Case L: a regional hospital's ransomware recovery 47
5.8 Case M: enel-med keeps care and data questions separate 48
5.9 Case N: SOP restoration and the business calendar 49
5.10 Case O: ePUAP and staged restoration 50
5.11 Case P: Autopay's recent access incident 51
5.12 What these cases do not add up to 51
5.13 Additional healthcare and industrial notices 52
5.14 Case Q: an industrial company separates encryption from possible copying 52
5.15 Case R: Żabka and an external supplier account 53
5.16 Case S: ZUS confirms a bounded availability event 54
5.17 Case T: Cyfrowy Polsat's April customer-data notice 55
5.18 Other notices retain narrower scope 55
5.19 Case V: retail mail-tool access and a larger data offer (B17) 56

15 detailed official-source case cards, separate from underground offers

CHAPTER 05

Confirmed incidents and claims by sector

IN SHORT

Healthcare software, accounting, education and public services provide the clearest official case material. Some notices confirm copied data; others confirm access while copying remains unresolved. Healthcare availability incidents add a separate recovery problem. The cases below retain those differences and do not create a national affected-person total. Start with your own supplier and account scope, then select the appropriate privacy, identity and continuity response.

5.1 Sector decisions

This table routes the evidence to the first responsible team. A sector's presence does not measure its share of national incidents.

Sector	Observed or reported activity	Evidence type	First response
Healthcare software	Historical records at MyDr; Medyc investigation; FELG patient-data access [S5] [S7][S8]	Official notices with different scope and certainty	Obtain practice-specific information and preserve the controller's risk decision
Healthcare delivery	Patient-data access at enelmed; ransomware at a regional hospital [S12][S35]	Provider and sector-authority reports	Separate patient communication from clinical continuity and recovery
Business software	Fakturownia confirms copying involving account, contractor and invoice information [S10]	Company confirmation	Rotate relevant access and independently verify payment changes
Education	University confirms copying and later publication; exact affected people unresolved [S41]	University confirmation	Review valid-account use and departmental data access
Government services	SOP restrictions and ePUAP staged restoration [S31] [S33][S34]	Official disclosures	Maintain alternative workflows and factual status communications
Payments	Autopay confirms access; copying and misuse remain unconfirmed [S45]	Company confirmation with explicit limits	Follow account-specific notices and monitor unauthorised transactions

Sector	Observed or reported activity	Evidence type	First response
Industry and services	Polish leak-site listings across several industry labels [S3]	Criminal claims	Validate any matching claim and test recovery independently
Energy and research	Historical energy report and a blocked research-institute attempt [S18][S43]	Official reports, different event dates and outcomes	Review remote management and safe process continuity

5.2 Case G: MyDr and historical medical records

CASE G

G

MyDr and historical medical records

Healthcare software

Official access account; potential population

OFFICIAL ACCOUNT	On 12 August the Ministry reported that the company confirmed unauthorised access to historical practice data through April 2024. It said the incident could concern 18.8 million people and more than 12,000 medical facilities [S5].
CHRONOLOGY	The August disclosure concerned older records. UODO issued controller guidance during the same period. Later UODO reporting described complaints and controller notifications, but those are separate units from potentially affected people [S6][S7].
WHAT IS ESTABLISHED	There was a company-confirmed access incident, as reported by the Ministry. The same statement said current care and prescription issuance were not disrupted. A continuing service therefore did not settle the confidentiality question.
WHAT REMAINS UNRESOLVED	The potential population is not a verified unique-person count held by this report. A later criminal offer cannot be assumed to contain the whole population or to originate from the same access.
ALTERNATIVE EXPLANATIONS TO TEST	An offered sample could be old, partial, combined with another source or falsely relabelled. Matching records should be assessed by the responsible controller through an authorised incident process.
RESPONSE	Medical practices should obtain their own scope from the processor and assess notification duties. Patient-support teams should use clear explanations and avoid asking people to submit sensitive records through an unverified contact.

Bottom line

Obtain practice-specific scope before adopting a population total.

5.3 Case H: Medyc and the boundary between investigation and scale

CASE H

H

Medyc and the boundary between investigation and scale

Healthcare software

Authority investigation; scale unverified

OFFICIAL ACCOUNT	UODO's 25 September notice says CBZC was investigating the incident involving Medyc software and that the regulator planned a Qbusoft inspection. It attributes the possible five-million-person figure to media reporting [S7].
WHAT IS ESTABLISHED	The authority publicly addressed the incident and the provider. Its notice is evidence of an official response, rather than independent validation of the advertised or reported dataset size.
WHAT REMAINS UNRESOLVED	The report does not establish a final unique-person count or that medical documentation for every user was copied. Different facilities can hold different information and receive different scope assessments.
ALTERNATIVES AND LIMITS	A central platform claim may describe one tenant, a subset of tables or a broader collection. The report does not resolve those possibilities from an advertisement alone. Repeated reporting of a figure is not a new measurement.
RESPONSE	A practice using the software should request an account-specific incident statement and preserve its own awareness timeline. Public communications should distinguish confirmed data categories from possible categories still being investigated.

Bottom line

An investigation and a media estimate are separate evidence.

5.4 Case I: FELG and provider claims about identity

CASE I

FELG and provider claims about identity

Healthcare software

Provider confirms access

OFFICIAL ACCOUNT	FELG's 1 October notice acknowledged access to patient data and reported a ransom demand. The statement attributed the claimed 10% share to the person claiming responsibility. It did not establish that percentage as its own completed assessment [S8].
CHRONOLOGY	A later update places the response to the received report on 29 September. The 7 October update says the company identified affected facilities and began sending individual information. The public sequence therefore distinguishes receipt, investigation and customer-specific notification.
WHAT REMAINS UNRESOLVED	The notice describes a person presenting as a group member. AHA's bulletin identifies an alias and treats the actor as distinct from earlier medical incidents. Neither account supplies this report with verified common-operator evidence [S8][S9].
ALTERNATIVES AND LIMITS	An alias may be genuine, borrowed or misleading. A sample or ransom demand does not establish the advertised fraction of a database or completed sale. The case is not used to join the medical incidents into one criminal organisation.
RESPONSE	A practice should use the individual scope provided by the processor and make its own controller assessment. A general instruction from a supplier does not replace the controller's decision under the law.

Bottom line

An affiliation claim does not establish a common operator.

5.5 Case J: Fakturownia and downstream payment fraud

CASE J

J

Fakturownia and downstream payment fraud

Business software

Company confirms copying

OFFICIAL ACCOUNT	The company states that unauthorised access ran from 27–28 September and that data were copied. Its expanded notice differentiates account information, integration material, contractor records and invoice information, with different date ranges [S10].
WHAT IS ESTABLISHED	This is a confirmed confidentiality incident. The provider also distinguishes data for which it is controller from data it processes for customers. The scope cannot be reduced to a single statement that all historical invoices or all recent information were taken.
WHAT REMAINS UNRESOLVED	No universal affected-person total is established here. The company states that payment-card details and bank login credentials were not stored by it. Payment information is therefore not interchangeable with card data or bank passwords.
ALTERNATIVES AND LIMITS	A convincing invoice scam after the notice could use this incident, another disclosure or legitimate business correspondence. A successful fraud is not demonstrated merely by the availability of accurate invoice details.
RESPONSE	Customers should complete the provider's relevant access changes and verify unusual payment instructions independently. Finance should call a contact known before the request. Security and privacy teams should preserve the customer-specific assessment.

Bottom line

Validate sensitive instructions using a previously trusted contact.

5.6 Case K: the University of Warsaw's changing assessment

CASE K

K

The University of Warsaw's changing assessment

Education

University confirms copying and publication

OFFICIAL ACCOUNT	The university states that access was detected on 9 February. Its later notice says data may have been copied during January–February and were published during the night of 15–16 April [S41].
WHAT IS ESTABLISHED	The later account confirms copying and publication. It describes use of valid credentials, most likely obtained through malware on a user's device. The university presents that origin as the likely explanation, not a forensic finding independently reproduced here.
UNITS MATTER	The published collection contained approximately 200,000 files and 850 GB. About 650 GB was public audiovisual material. Approximately 32,800 files may have contained personal data. These are files and storage volumes, not numbers of affected people.
WHAT REMAINS UNRESOLVED	The university did not identify every affected individual in the notice. It said key systems were not disrupted or encrypted. Absence of encryption did not mean absence of a confidentiality incident.
RESPONSE	Universities should examine valid-account access and departmental repositories together. Incident records should preserve superseded assessments, showing why the conclusion changed. A February statement should not override a later, more specific disclosure.

Bottom line

File counts are not affected-person counts.

5.7 Case L: a regional hospital's ransomware recovery

CASE L

L

A regional hospital's ransomware recovery

Healthcare

Official encryption and recovery account

OFFICIAL ACCOUNT	A 25 March sector-authority article describes ransomware on 8 March at a regional hospital. Some resources were encrypted, access to information was limited and the hospital moved to emergency working arrangements [S35].
WHAT IS ESTABLISHED	The hospital spokesperson describes disruption and a recovery expected to take weeks. The account explicitly does not describe complete paralysis. On-site and remote response support involved several national and sector teams.
WHAT REMAINS UNRESOLVED	The article identifies a confidentiality risk, but does not provide a final exfiltration or affected-person total. It does not justify attaching a particular extortion group to the event without additional evidence.
RESPONSE	Hospitals should test the clinical workflow during limited data access. A restore test should include current patient work, safe manual records, reconciliation and business acceptance. A successful backup task alone does not demonstrate those capabilities.

Bottom line

Accept recovery only after the clinical workflow works.

5.8 Case M: enel-med keeps care and data questions separate

CASE M

M

Enel-med keeps care and data questions separate

Healthcare

Provider confirms access; scope estimated

OFFICIAL ACCOUNT	The provider's 27 September notice says it detected access to part of its infrastructure and patient data on 24 September. It said the incident might concern around 3% of its patient database [S12].
WHAT IS ESTABLISHED	The provider acknowledges access and individual notification. It also states that facilities continued operating normally. The percentage is its estimate, with no denominator in the notice that would support conversion into a number of people.
WHAT REMAINS UNRESOLVED	This report does not infer that all patients, every data category or all provider systems were affected. It does not join the event to another healthcare incident through proximity in time.
RESPONSE	Use individual notifications and verified provider contacts. Prepare staff for fraud calls citing genuine patient details while maintaining the distinction between continued care and the data investigation.

Bottom line

Continued care and a confidentiality investigation can coexist.

5.9 Case N: SOP restoration and the business calendar

CASE N

N

SOP restoration and the business calendar

Government

Official incident; data scope under analysis

OFFICIAL ACCOUNT	The Ministry of Culture reports a 6 October incident in the grant-programme system SOP. Its 9 October notice says the system was isolated and user informa- tion may have been accessed; the data scope was still under analysis [S33].
CHRONOLOGY	On 28 October the Ministry linked delayed 2027 programme calls to restoration work. It said data entered through 5 October had been restored from backups. Restored data and restored full service are separate statements [S34].
WHAT REMAINS UNRESOLVED	A count of registered users would not establish the number whose personal data were copied. The notice does not attribute the event to a state, group or criminal market advertisement.
RESPONSE	Public and private grant systems should preserve submission evidence and communicate revised workflow arrangements. Recovery acceptance must include the actual application process and its deadlines, rather than database restoration alone.

Bottom line

Restore the application workflow and its submission evidence.

5.10 Case O: ePUAP and staged restoration

CASE O

EPUAP and staged restoration

Government

Official staged restoration

OFFICIAL ACCOUNT	On 19 November the Ministry of Digital Affairs announced full restoration after an incident detected on 10 November. It described precautionary restrictions, analysis, additional safeguards and testing before reopening components [S31].
CHRONOLOGY	The same notice records an interim solution on 15 November and all transactional services through the specified public-service portal operating on 16 November. Full ePUAP operation followed on 19 November.
WHAT REMAINS UNRESOLVED	The announcement does not establish the attack method, actor or a personal-data theft total. It also says investigators found no traces of expansion beyond the identified area. This is the Ministry's reported finding, within that investigation.
RESPONSE	Organisations that depend on electronic submissions should test an authorised alternative and retain proof of attempts and completion. Communications should distinguish limited access, partial restoration and full operation.

Bottom line

Distinguish partial restoration from full service.

5.11 Case P: Autopay's recent access incident

P

CASE P

Autopay's recent access incident

Payments

Access confirmed; copying unresolved

OFFICIAL ACCOUNT	Autopay says it detected unauthorised access to infrastructure and part of its processed-payment information on 11 November. It says copying or use of the data was not confirmed, while remaining unable to exclude it [S45].
WHAT IS ESTABLISHED	The provider blocked access and describes direct communication with potentially affected customers. PRNews reported the notice during the same recent period. No affected-person total is supplied by the sources used here [S46].
ALTERNATIVES AND LIMITS	Access, copying and later misuse are separate propositions. Neither an actor advertisement nor a social-media summary should remove the company's explicit uncertainty. This report does not infer a loss of card data.
RESPONSE	Customers should follow verified account-specific instructions and report unauthorised transactions through their bank's established channel. Support teams should expect impostors to cite the real incident when requesting codes or urgent action.

Bottom line

Use account-specific notices and established bank channels.

5.12 What these cases do not add up to

The fifteen detailed cases are dossiers with different evidence and units. They do not establish a complete national incident count. Several concern access without a confirmed final population; others concern continuity without a published data-theft finding.

The report does not add patient estimates, university files, platform accounts or ransomware listings. People may appear in several providers' records. Public announcements may also describe the same event at several stages.

5.13 Additional healthcare and industrial notices

Three additional March healthcare notices describe encryption or unavailable records. One provider identified ransomware on 13 March; another reports an event on 24 March; a rehabilitation provider identified it on 31 March. Their statements retain qualifications about possible or probable data acquisition [S56][S57][S58].

The 24 March notice reports recovery of access to records created through 24 June 2021. That wording does not establish permanent loss of newer records. An adjacent historical paper-record notice at another provider is also excluded from this year's ransomware population.

In early November, an official sanitary warning included Poland in a refrigeration-control campaign. PAP quoted the CERT head confirming one Polish device incident, without material loss after the operator intervened. The wider exposed-device population is a different measure [S54][S55].

These notices add specific continuity and industrial-control lessons. They remain mentions, rather than additional detailed case cards. No operator is assigned to a state or criminal group by this report.

5.14 Case Q: an industrial company separates encryption from possible copying

CASE Q

An industrial company separates encryption from possible copying

Industry

Encryption confirmed; copying unresolved

OFFICIAL ACCOUNT	An industrial company says it detected ransomware on 29 October, with a possible start on 28 October. It confirms encryption of some data and loss of access. Its notice says copying and publication remain unconfirmed [S71].
CHRONOLOGY	The notice history gives first publication on 3 November and an expanded update on 19 November. The heading displays 10 November. These are disclosure-page dates, rather than three separate attacks.
WHAT REMAINS UNRESOLVED	The company was still establishing the data, people and periods involved. Its stated risk of access does not supply a verified affected-person total or evidence that a sale occurred.
RESPONSE	Use the appropriate notice for the affected relationship and verify unusual instructions independently. Recovery and privacy teams should track access restoration, data integrity, possible copying and individual notification separately.

Bottom line

Track data integrity, access restoration and privacy scope separately.

5.15 Case R: Żabka and an external supplier account

CASE R

R

Żabka and an external supplier account

Retail

Supplier-account access confirmed

OFFICIAL ACCOUNT	Żabka's 4 August statement confirms unauthorised access through an external supplier account. It concerns selected technical resources supporting exchange between the franchisor and franchisees. The company says it detected the access late in the preceding week and blocked it [S72].
WHAT IS ESTABLISHED	The company acknowledged a specific supplier-account route. It stated that transactional data, consumer services, Żappka confidentiality and operations remained intact. Those statements do not validate every separate seller assertion about technical files or repositories.
WHAT REMAINS UNRESOLVED	This report establishes no affected-person total, completed sale or correspondence between every advertised object and the official scope. Technical-resource counts should not be presented as customer counts.
RESPONSE	Review supplier identities, permitted resources and emergency revocation. Ask the service owner to test whether access removal actually covers tokens, sessions and delegated applications. Preserve the supplier-specific investigation rather than assuming every consumer service was involved.

Bottom line

Validate supplier identities, sessions and emergency revocation.

5.16 Case S: ZUS confirms a bounded availability event

CASE S

S

ZUS confirms a bounded availability event

Public services

DDoS availability incident confirmed

OFFICIAL ACCOUNT	ZUS's 10 August notice says a volumetric DDoS attack before midday affected access to its website and could also affect eZUS. The notice announces restored login. It explicitly states that ZUS and customer data were not threatened [S73].
WHAT REMAINS UNRESOLVED	The notice does not provide an attacker attribution, a detailed interruption duration or a business-loss total. Its availability account should not be rewritten as a personal-data theft incident.
RESPONSE	Public-service owners should test the external mitigation decision, customer alternatives and the actual login workflow. Communications should state the bounded service impact and the evidence supporting any statement about data.

Bottom line

Test service restoration and preserve the data-impact boundary.

5.17 Case T: Cyfrowy Polsat's April customer-data notice

CASE T

T

Cyfrowy Polsat's April customer-data notice

Telecommunications

April customer-data access confirmed

OFFICIAL ACCOUNT	Cyfrowy Polsat's notice explicitly supplements information dated 29 April 2026. It concerns unauthorised access to part of its customer information during April. The company says monitoring had not detected publication [S74].
WHAT IS ESTABLISHED	The notice lists possible identity and contact categories. It says technical safeguards were not broken and excludes customer logins, passwords and payment-card information. The company's characterisation of the access mechanism remains its own account.
WHAT REMAINS UNRESOLVED	No universal affected-person count is established here. A separately advertised portal-access claim is not joined to this event without evidence. The date of reading an updated page is not a new incident date.
RESPONSE	Customer support should distinguish identity-data risks from password or card incidents. Use verified company guidance and the person's actual scope. Knowledge of identity details should not authorise a sensitive account change.

Bottom line

Follow person-specific scope and verified identity-protection guidance.

5.18 Other notices retain narrower scope

A teaching hospital's 10 March notice concerns employee-mailbox access detected on 2 March. It says the correspondence included patient information, while misuse and publication were unconfirmed. It does not establish a service outage or an affected-person total [S78].

A separate hospital notice describes a 27 February internal access-control failure: an employee left an unauthorised former employee with an already logged-in workstation. The notice does not establish that records were viewed. This is a privacy and access-control example, not a confirmed remote cyberattack [S79].

A retail outlet operator's March notice confirms access and traces of limited file downloading. Its visible date is 10 March, while metadata gives 11 March. Neither date establishes when the access began. The scope requires relationship-specific assessment [S80].

A recreation operator's signed 4 November notice confirms a few minutes of unauthorised camera viewing on 22 October, discovered on 28 October. It reports no access to the local network or other customer data and no evidence of image downloading. This bounded event does not establish broader surveillance [S81].

A medical controller separately reports effects of an unnamed software-provider incident in August and September. It distinguishes confirmed confidentiality effects, highly likely file theft and unresolved categories. Its notice does not identify the provider or establish continuous access by one actor [S77].

September reporting by a public broadcaster relays a travel intermediary's statement about customer-information access, including identity and travel-document details. A standalone primary notice was not located in this review. Retain this as qualified reporting, without treating it as the same event as an underground travel advertisement [S76].

5.19 Case V: retail mail-tool access and a larger data offer (B17)

Evidence card B17 23 Jan 2026

Spirigatito | Forum | Forum | English

ORIGINAL

487 837 unique users

Held

The advertiser claims 1,528,945 lines including tickets and 487,837 unique users; contact and support-message schemas are retained.

Not established

The advertised files, totals, acquisition date and their match to the official mail-tool notice are unverified.

CASE V

V

Retail mail-tool access and a larger data offer

Evidence card B17 | 23 Jan 2026 | Forum | Retail customer service

Official mail-tool notice; offer totals unverified

ADVERTISED SCOPE	Two forum advertisements dated 23 January claim 1,528,945 lines, including support tickets, and 487,837 unique users associated with a Polish retail business. These are the seller's units, not verified people. They represent one advertised offer, without establishing separate intrusions [S1].
OFFICIAL SCOPE	The business reports detecting access to correspondents' email addresses on 23 January. Its 13 February update confines the incident to a mail-handling tool and excludes online-shop, order and payment data [S89].
WHAT IS HELD	The retained advertisements contain contact and support-message schemas, alongside examples whose personal values are withheld. A later

reply says the incident was confirmed. The company's notice supports a narrower access event, without verifying the advertised files or totals.

WHAT REMAINS UNVERIFIED	The seller's line and user totals, the advertised files' authenticity, the acquisition date and unique people are unestablished. The report does not establish that the offered database is the material described in the official notice.
RESPONSE	Review mail and support-system access with identity and privacy owners. Check unusual exports, account changes and misuse of genuine ticket details. Validate scope before adopting a customer-population figure or accepting a support-themed instruction.
	> [!TAKEAWAY] A confirmed access incident can still have unresolved copying and population figures. ;; Recovery must restore the business workflow, not just the database. ;; Use the latest specific official account while preserving the earlier chronology.

Bottom line

Keep the official access scope separate from the advertised database totals.

CHAPTER 06

Hacktivism, DDoS and recent activity

06

THIS CHAPTER ANSWERS

What separates a politically framed claim from an established service event?

9–22 November

recent-activity focus within the full-year window

6.1 DDoS claims need their own evidence 59

6.2 Claim versus reporting 59

6.3 Timeline of claims, campaigns and official updates 60

6.4 Recent activity: 9–22 November 61

6.5 Communications that preserve uncertainty 62

CHAPTER 06

Hacktivism, DDoS and recent activity

IN SHORT

Politically framed DDoS claims form one evidence track. Official November notices about public services and payments form another. The ePUAP recovery statement does not identify a DDoS group or confirm data theft. Autopay confirms access while leaving copying unresolved. Maintain availability measurements, a trusted status channel and an incident-specific assessment before connecting claims to service events.

6.1 DDoS claims need their own evidence

ZeroFox reports observing NoName057(16) and DarkStorm Team claims involving Polish organisations on 12 January. The researcher describes the groups and their political framing. This report attributes those descriptions to ZeroFox [S30].

The observation establishes that claims were published. A target list, screenshot or external availability check does not establish the duration, geographic reach or business impact of an interruption. It also does not establish state direction.

Country references and statements about Ukraine, Russia or Belarus should not become explanations adopted by the publisher. A claimant's rationale is its own account. Defenders can use a newly named target as a readiness signal without endorsing the narrative.

Energetyka24 relays an energy-sector organisation's statement describing a brief website interruption and no reported impact on operational services [S75]. A standalone primary notice was not available for verification. This reporting does not establish state direction.

6.2 Claim versus reporting

The panel concerns the January claims only. It does not link those claims to the November incidents.

Point	Actor claim	Official account	Public research
Activity	DDoS against Polish organisations, as relayed in research	No target-specific official confirmation established here	ZeroFox reports observing the claims on 12 January [S30]
Impact	Claimed interruption	No supported duration or business-loss measure	Publication of a claim is not independent service telemetry
Attribution	Group names attached to announcements	No state attribution established by this panel	Political alignment is ZeroFox's description, not a conclusion from language
Defender decision	Validate the named service	Ask the operator for its own service facts	Preserve claim time, provider measurements and response decisions separately

The absence of an official match does not establish that a claim was fabricated. It sets the boundary of this report's knowledge. A public update should explain what the organisation can verify rather than repeat the group's impact language.

A retained 13 September NoName057(16) post also claims activity against public-service and commercial sites. Its target entries and availability links do not establish verified outages (B07) [S1].

Evidence card B07 — 13 Sep 2026

NoName057(16) | Telegram channel | Telegram | English

ORIGINAL

Poland [...]

Note. Target list and rhetoric omitted. Only the country reference is quoted.

Held

A retained actor post claims activity against Polish public-service and commercial sites.

Not established

Service disruption, duration, impact, attack traffic and attribution beyond the display alias are unverified.

6.3 Timeline of claims, campaigns and official updates

Dates refer to the event or publication stated in each row. An official update is not automatically a newly occurring incident.

12 Jan 2026 — **Public research**

ZeroFox observes claims by NoName057(16) and DarkStorm Team involving Polish organisations [S30]

12 Jun 2026 — **CERT Polska**

Reports Gmail phishing attributed to UNC1151/Ghostwriter, active from March [S14]

23 Sep 2026	**CERT Polska** Publishes analysis of Polish-targeted mobile toll fraud [S15]
10 Nov 2026	**Ministry of Digital Affairs** Incident date later given for ePUAP restrictions [S31]
11 Nov 2026	**Payment provider** Autopay detects unauthorised access; copying remains unconfirmed [S45]
15 Nov 2026	**Ministry of Digital Affairs** Interim solution restores substantial public-service functionality, according to the later notice [S31]
18 Nov 2026	**CERT Polska** Publishes nVision token-handling advisory [S23]
19 Nov 2026	**Ministry of Digital Affairs** Announces full ePUAP restoration after staged testing [S31]

6.4 Recent activity: 9–22 November

Public-service restoration has several milestones. The ePUAP notice distinguishes detection on 10 November, an interim solution on 15 November, transactional services on 16 November and full operation on 19 November. It does not assign a group or announce a confirmed personal-data theft total [S31].

For dependent organisations, the immediate question is whether the required submission or customer workflow can be completed. A homepage becoming reachable is insufficient evidence of that. Keep records of the authorised alternative, attempted submissions and eventual acceptance.

Payment-data access retains a copying boundary. Autopay's notice concerns detection on 11 November. It confirms access but explicitly does not confirm copying or misuse. PRNews places the public communication in the same recent period [S45][S46].

Customer-support teams should provide verified instructions and a safe callback process. An impostor may cite the genuine notice. Knowledge of the event does not authorise requests for codes, account changes or transfers.

A recent advisory creates a patch decision. CERT Polska's 18 November nVision notice describes a user token carried in a URL query. It identifies versions below 18 as affected and version 18 as fixed. NVD's record also identifies the fix [S23][S24].

This is a vulnerability disclosure, not a count of affected Polish organisations or confirmed exploitation. Owners should establish whether they use the product, update where applicable and assess relevant token exposure through their own logs.

The final day is partial. The cut-off is 22 November, but observations were made during that date. The report cannot include posts or notices that had not yet appeared when read. November is not compared with a full month as a measure of threat intensity.

Recent advertising remains unverified. A 16 November forum offer prices a purported public-body mailbox at USD 550 and claims current inventory. A 15 November food-service offer claims a fresh export. These are recent advertisements, without established access, freshness or a link to ePUAP or Autopay (B08, B03) [S1].

An industrial update concerns an earlier event. An industrial company expanded its notice on 19 November about ransomware detected on 29 October. Encryption and lost access are confirmed; copying and publication remain unresolved. The recent development is a disclosure update, rather than a new attack [S71].

A multinational offer includes a Poland label. A 12 November advertisement offers country-labelled data packages, including Poland. It claims about 103–255 GB per country package. Authenticity, actual country composition, acquisition date and unique people remain unverified. Related promotions on 14 and 16 November are not additional incidents (B16) [S1].

The label does not establish a new Polish corporate intrusion or a connection to the official November notices. The advertised package size is a seller assertion, rather than a measured Polish data population.

Evidence card B16 12 Nov 2026

Suction19213821 Forum Forum English

ORIGINAL

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

Held

A multinational offer includes a Poland-labelled package and claims country-package sizes.

Not established

Authenticity, country composition, size, provenance, current access and unique people are unverified.

6.5 Communications that preserve uncertainty

A useful first statement identifies affected services, the current restriction, an alternative channel and the next update time. It should state separately whether access, copying, publication and misuse are established or still being investigated.

Avoid declaring a national campaign from similar timing or political themes. A security incident at a payment provider and a restricted public-service platform do not become one operation without a concrete evidential link.

For DDoS readiness, agree the provider contact, mitigation decision-maker, service measurements and spokesperson. An exercise should test both activation and the public account of impact. The completion evidence is a functioning decision process and retained measurements.

KEY TAKEAWAYS

01

A published claim and a service interruption require separate verification.

02

November access and restoration notices retain their own unresolved questions.

03

Prepare mitigation, alternative workflows and factual communications before the next claim.

CHAPTER 07

Threat actors and evidence relationships

THIS CHAPTER ANSWERS

Which actor propositions are supported, and which relationships should remain unconnected?

56

Polish ransomware listings under 21 group labels

7.1 Relationship map: evidence before a connecting line 65
7.2 UNC1151/Ghostwriter: a current mailbox campaign 66
7.3 Behaviour matrix for the mailbox campaign 67
7.4 DDoS claimants 68
7.5 Ransomware: a visible listing population 69
7.6 Historical vendor context without a new Polish case 72
7.7 Criminal personas and common-operator claims 73
7.8 DKWOC's targeted document campaign 73
7.9 Target lists and historical campaign dates 73

CHAPTER 07

Threat actors and evidence relationships

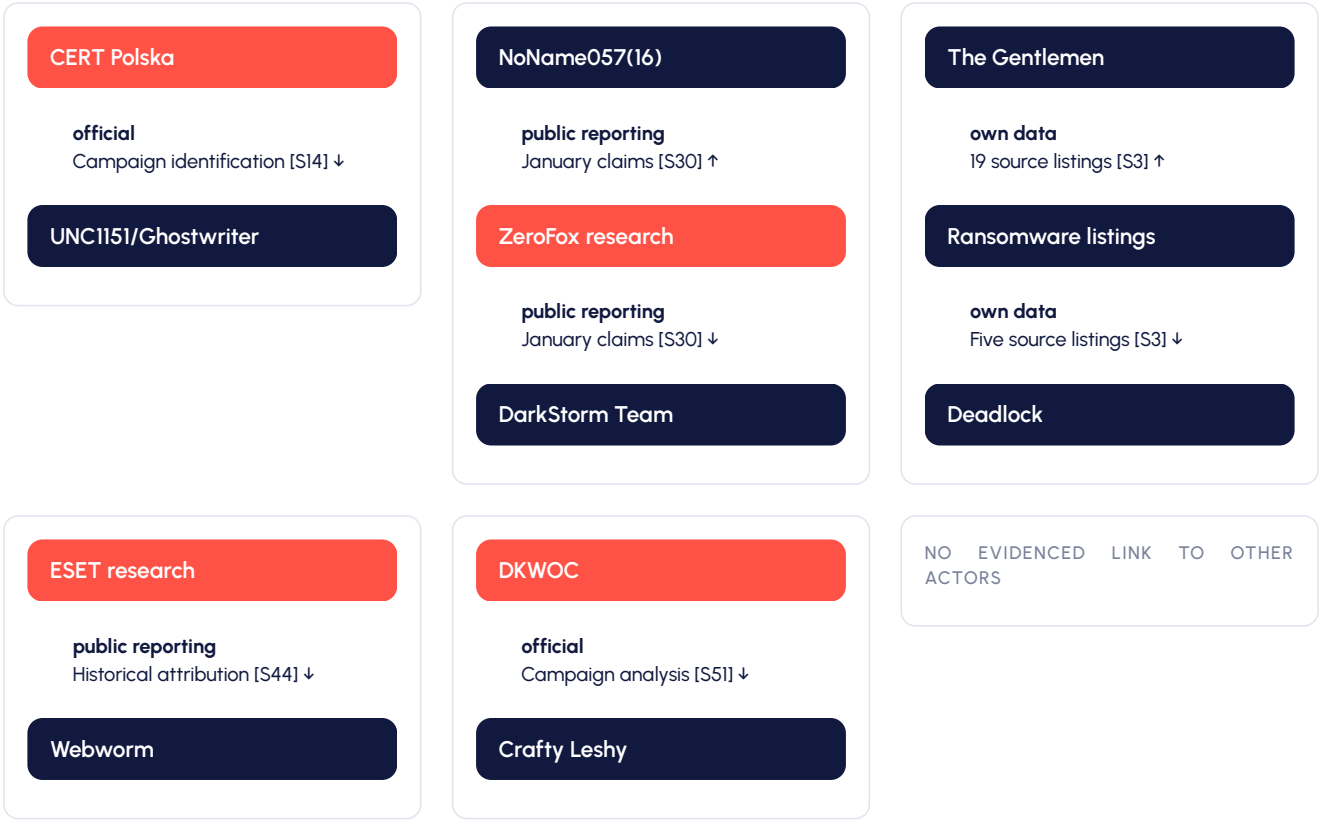
IN SHORT

CERT Polska attributes a current phishing campaign to UNC1151/Ghostwriter. Public research describes DDoS claims and historical espionage context. Ransompedia records 56 Polish listings, with The Gentlemen the largest group label. These sources describe different populations and do not establish a single operating network. Select controls from the observed behaviour and preserve each source's attribution boundary.

7.1 Relationship map: evidence before a connecting line

The map distinguishes official attribution, public research and listing observations. It does not draw a link between actors merely because they mention Poland, use the same language or appear during the same month.

Own post · Relay · Official statement · Public reporting · Our observation



Relationship	Evidence	What it supports	What it does not support
CERT Polska to UNC1151/ Ghostwriter campaign	Official research [S14]	The source's campaign identification and described behaviour	A victim count or an independent state-attribution finding
ZeroFox to NoName057(16) and DarkStorm Team claims	Public research [S30]	Observation of January announcements	Verified business impact or a link to November incidents
Ransompedia to The Gentlemen label	Listing observation [S3]	Nineteen Poland-labelled listings in the snapshot	Proof that every listing reflects encryption or the same operator
ESET to Webworm	Vendor research [S44]	ESET's identification and China-alignment assessment of a chiefly 2025 campaign	A newly confirmed Polish intrusion in 2026

No concrete evidence in those relationships links the phishing campaign, DDoS claimants and extortion listings into one organisation. A planning model that connects an access seller, data holder and fraud user would be an analytical model, not an established criminal supply chain.

7.2 UNC1151/Ghostwriter: a current mailbox campaign

CERT Polska's June account says Gmail targeting began in March 2026. The messages impersonated security notices, used Polish-language pressure and sought passwords and second-factor codes. The described target roles include public administration, researchers, journalists and people connected to them [S14].

The source reports both dedicated phishing sites and abused web services. It also describes information sought after mailbox access, including contacts, sensitive documents and associated accounts. This supports a defence focused on sign-in authority and mailbox activity.

It does not demonstrate that every message reached its intended person or that every attempted login succeeded. The report does not assign the campaign to a state independently, nor infer that a person's public role establishes that they were a selected target.

UNC1151/Ghostwriter

Mailbox phishing campaign | Campaign identification by CERT Polska; no independent state attribution

IN POLAND, 2026

March 2026
Gmail campaign begins, according to CERT

12 June 2026
Official campaign analysis published

CLAIMED TARGETS

Roles and connected people described by CERT Polska

SEEN IN PUBLIC REPORTING

[S14] Official campaign description

OUR ASSESSMENT

Validate sign-ins and mailbox activity. Second-factor codes are part of the described phishing route.

CONFIDENCE

High for the official account; outcomes need account-specific evidence

7.3 Behaviour matrix for the mailbox campaign

This is Odin's analytical mapping of the behaviours described by CERT Polska to MITRE ATT&CK. It is not a claim that CERT supplied these identifiers. Technique definitions were read at MITRE [S47][S48][S49][S50].

ANALYTICAL MAPPING OF MAILBOX CAMPAIGN BEHAVIOURS TO MITRE TECHNIQUES

Initial access	Credential access	Account use	Collection
T1566.002 Phishing link	T1111 Second-factor interception	T1078 Valid accounts	T1114.002 Remote email collection

Odin's analytical mapping of behaviours described by CERT Polska to MITRE definitions. Not a source-supplied mapping or a tested detector. [S14]

Behaviour	ATT&CK	Source-supported scope	Defensive question
Link in a security-themed phishing email	T1566.002	Described delivery route [S14][S47]	Can a recipient report the lure without following it?
Interception of a second-factor code	T1111	Described code collection and login attempt [S14] [S48]	Are high-impact sign-ins resistant to credential relay?
Use of obtained credentials	T1078	Described attempt to access the real account [S14][S49]	Can suspicious account use be correlated with session activity?
Search of an accessed mailbox	T1114.002	Described collection purpose; no national success count [S14][S50]	Do mailbox access and export records reach the response team?

This matrix is a validation guide, not a detection rule or a tested coverage claim. It should be translated into the organisation's own telemetry and exercised before being described as operational detection.

7.4 DDoS claimants

The NoName057(16) and DarkStorm Team descriptions derive from ZeroFox's research. The source's political characterisation remains attributed to it. The report uses the January observations to motivate service readiness, not to assign responsibility for every Polish outage [S30].

NoName057(16)

DDoS claimant | Described as pro-Russia by ZeroFox; no state direction established

IN POLAND, 2026

12 January 2026
Claims observed by ZeroFox

13 September 2026
Retained claim concerning Polish sites (B07)

CLAIMED TARGETS

Generic public-service and commercial sites, identifiers withheld

IN THEIR WORDS

"Poland [...]" B07

SEEN IN PUBLIC REPORTING

[S1] Retained post B07

[S30] Public research on January claims

OUR ASSESSMENT

An announcement and availability links do not establish duration, business impact or responsibility for November incidents.

CONFIDENCE
High that the claim was retained; impact unverified

DarkStorm Team

DDoS claimant | No independent state attribution in this report

IN POLAND, 2026

12 January 2026
Poland-related claims observed in public research

CLAIMED TARGETS

Organisations described in the cited research

SEEN IN PUBLIC REPORTING

[S30] January observations

OUR ASSESSMENT

Use operator measurements before adopting an impact claim. No relationship to November incidents is established.

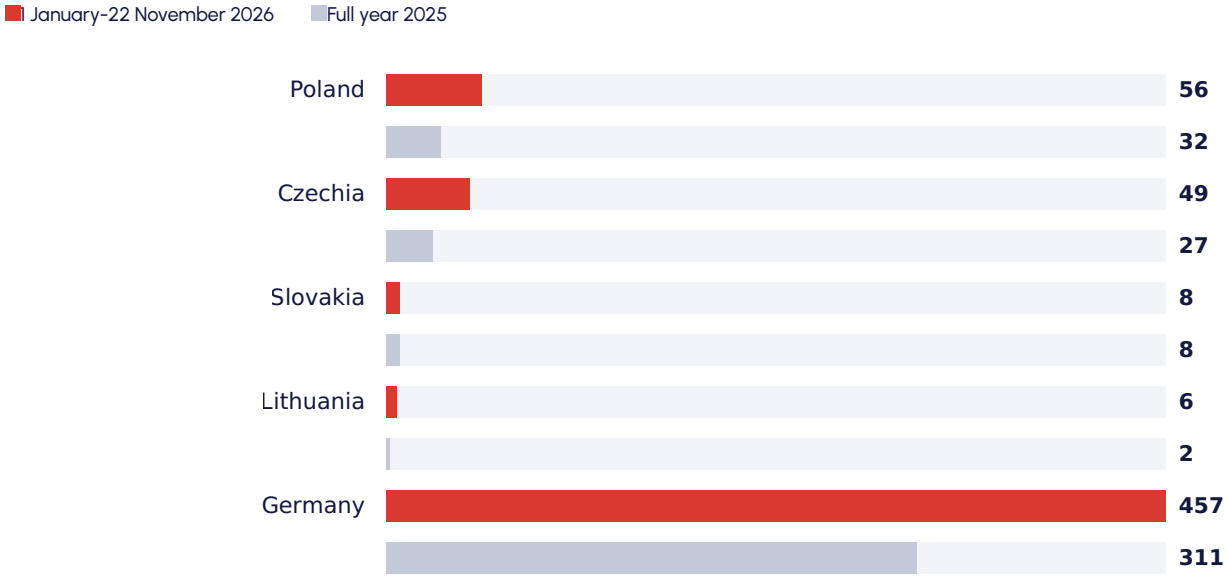
CONFIDENCE
As scoped by ZeroFox

An organisation should not use the actor's preferred language as its own public explanation. Confirm the actual affected workflow, mitigation status and restoration milestone. A service-provider measurement is stronger impact evidence than a claimant's screenshot.

7.5 Ransomware: a visible listing population

Ransompedia records 56 Poland-labelled listings during the stated 2026 window and 32 during the whole of 2025. The periods differ. This is not an annual growth rate, a count of confirmed victims or a measure of national attack probability [S3].

Regional listing totals describe visibility, not country risk



Source: Brandefense Ransompedia listing snapshot. 2026: 1 January–22 November; 2025: full year. Unmatched periods; not a national risk ranking [S3].

Comparison countries were selected as examples to provide context only; they do not imply a ranking or political assessment.

Country	2026 window	Full 2025	Interpretation
Poland	56	32	Partial year compared with a complete year
Czechia	49	27	Adjacent industrial and service economy
Slovakia	8	8	Smaller adjacent manufacturing and transport economy
Lithuania	6	2	Nearby Baltic service and logistics peer
Germany	457	311	Larger adjacent economy; totals are not size-adjusted

The four peers were chosen for geography and service dependencies. They are not a political grouping. Country labels follow the source snapshot and may require organisation-level verification; the report does not use them to rank national security.

The largest Polish group labels are The Gentlemen with 19 listings, Deadlock with five, Coinbasecartel and Nova with four each, and Qilin with three. Sixteen further labels account for 21 listings. The largest label therefore represents 33.9% of the 56 observations.

The Gentlemen

Ransomware listing label | Extortion claims; no state attribution

IN POLAND, 2026

2026 window

19 Poland-labelled listings

CLAIMED TARGETS

Several industry labels; no public victim list

SEEN IN PUBLIC REPORTING

[S3] Nineteen of 56 Polish listings

OUR ASSESSMENT

The largest listing label in this source snapshot. The label does not prove common operators or encryption in every case.

CONFIDENCE

High for source counts, not underlying outcomes

Deadlock

Ransomware listing label | Extortion claims; no state attribution

IN POLAND, 2026

2026 window

Five Poland-labelled listings

CLAIMED TARGETS

Source-assigned industry categories

SEEN IN PUBLIC REPORTING

[S3] Five of 56 Polish listings

OUR ASSESSMENT

Prepare group-independent recovery and validate any matching claim.

CONFIDENCE

High for source counts

Monthly Polish counts sum to 56. July contains ten listings, April eight and January seven. November has three at the snapshot and is partial. Those dates refer to listing publication or the source's fallback date, not the intrusion start.

Grouped industry labels describe 17 technology-related listings, 13 industrial listings, eight education listings, seven consulting listings and eleven in other sectors. These are listings, not independently counted organisations. They are not joined to the selected-domain sample.

7.6 Historical vendor context without a new Polish case

ESET's May 2026 research describes Webworm's 2025 activity and identifies Polish government targeting among several European countries. ESET calls the group China-aligned and describes cloud-service command channels and proxy tools [S44].

The source also describes activity extending into January 2026 involving a Spanish entity. That detail does not establish a Polish intrusion in January. The report retains the Polish targeting as historical context disclosed in 2026.

Webworm

Historical espionage context | China-aligned, according to ESET

IN POLAND, 2026

2025 activity

Polish government targeting described in May 2026 research

CLAIMED TARGETS

Government organisations in several countries

SEEN IN PUBLIC REPORTING

[S44] Research on cloud-service command channels and proxies

OUR ASSESSMENT

The source mainly concerns 2025. The report does not infer a new Polish January 2026 intrusion from activity involving another country.

CONFIDENCE

As attributed and dated by ESET

For defenders, the useful question is whether servers make unusual use of cloud messaging, file-sharing and proxy services. The vendor's group attribution should not replace local validation of legitimate applications and administrative activity.

7.7 Criminal personas and common-operator claims

An alias is a label on an advertisement or statement. Matching names do not prove a legal identity, while different names do not prove different people. Claims about a medical-provider incident and a business-software incident should be linked only at the level supported by evidence.

FELG's notice and AHA's account illustrate why caution matters: the person claimed an affiliation, while public research described a different actor. This report retains both accounts and does not resolve common ownership from branding [S8][S9].

The post cards preserve the original claim language only where it adds defensive value. Contacts, target identifiers and political rhetoric are removed. Shared advertising supports an advertising relationship; it does not prove a shared file, access path or completed transaction.

7.8 DKWOC's targeted document campaign

DKWOC describes identifying campaign artifacts on 30 January 2026 involving domestic and foreign institutions. It tracks the activity as Crafty Leshy and reports CERT-UA's mapping to UAC-0001/APT28. Both identifiers remain source-specific assessments [S51].

The official account describes institution-themed messages sent through previously accessed mailboxes and malicious Office documents. It does not provide a Polish victim total. Its exact publication date is not exposed in the available primary page, so the report uses its explicitly stated observation date.

For CVE-2026-21509, NVD lists affected Office product families. Microsoft's advisory gives separate protections for older releases and service-protected editions. The verified version details are in Appendix A; merely opening the advisory is not evidence that an organisation applied the fix [S52][S53].

7.9 Target lists and historical campaign dates

ThreatFabric's 20 August Manic analysis explicitly includes Poland in its banking and government-identity application targets. Infrastructure dates reach back to February, while retained components appear later. The target list establishes intended application coverage, without a Polish infection count or evidence of access to bank infrastructure [S86].

Group-IB's 23 September RemControl analysis includes Poland in its financial overlay targeting. Its detailed delivery example and campaign labels concern other geographies. A supported Polish overlay does not establish that the observed delivery reached Polish users; no local victim count is supplied [S87].

Unit 42's February Shadow Campaigns publication places the Polish government targeting in 2025. Its separate January activity concerns another country. It is historical context, not a newly established Polish 2026 incident. The research labels and state-alignment assessment remain Unit 42's, rather than this report's independent attribution [S88].

KEY TAKEAWAYS

01

Tie every actor description and state assessment to its source.

02

Choose controls from behaviours and local validation, not group branding.

03

Keep listing labels, persona claims and confirmed incidents as separate evidence populations.

CHAPTER 08

The fraud economy

08

THIS CHAPTER ANSWERS

How can identity information become a fraudulent instruction or charge?

3

separate validation questions: identity, authority and transaction

8.1 Information and authority are different assets 76
8.2 Payment-card material: narrow scope 76
8.3 Account trading and identity documents 76
8.4 Mobile fraud includes more than card checkout 77
8.5 Business email and payment changes 77
8.6 Price language is not market value 77
8.7 A practical fraud-response hand-off 78
8.8 Official campaign observations across the year 78
8.9 Campaign and enforcement context 79

CHAPTER 08

The fraud economy

IN SHORT

A believable message can contain genuine personal or business information without having genuine authority. Official disclosures and mobile-malware research show why account recovery, payee changes and support calls need independent checks. Underground advertisements describe supply and demand, not completed transactions or national losses. Keep payment-card material within its narrow scope and test the business decision an impostor is trying to change.

8.1 Information and authority are different assets

A name, address, health reference or accurate invoice can make a message convincing. It cannot establish that the sender is a bank, medical provider or legitimate supplier. The MyDr, university and accounting disclosures make that distinction operationally relevant [S5][S10][S41].

An incident notice may itself become a pretext. A caller can cite a real event and offer to protect an account, verify a patient or move money. Staff should recognise the event without granting authority to the caller.

The first question is whether the interaction was initiated through a trusted route. The next is whether the person has authority for the requested action. A final check confirms the transaction or data disclosure. Combining those questions into a quiz about personal details creates a weak decision point.

8.2 Payment-card material: narrow scope

SCOPE OF THE CARD FIGURES

The figures cover only payment cards that appeared in clear text in dark-web posts collected for this report. Brandefense detects stolen cards through many other methods outside this report. These figures do not measure card theft or fraud loss.

The retained posts contain 455 distinct Poland-associated cards across 413 posts. Of these, 76 are issuer-associated and 379 country-only. These groups are disjoint. No issuer-level table is published, and account validity, successful payments and losses are not established [S4].

8.3 Account trading and identity documents

An advertisement offering an account or identity package is evidence of an offer. It does not establish that the account is active, the documents are genuine, the seller controls the account or the transaction was completed. The post cards retain these limits [S1].

For defenders, the relevant route is often account creation or recovery. A service should ask how an applicant's identity is verified, how a new device is approved and who can override a failed check. A stolen document image should not become sufficient authority by itself.

SIM and telephone recovery also need joint ownership. Customer support, identity teams and telecommunications providers can hold different parts of the evidence. A synthetic exercise should show whether the organisation can stop an unusual recovery without permanently excluding a legitimate customer.

A retained rental-fraud recruitment advertisement describes a Poland-focused workflow involving advance document, insurance and reservation payments. It is evidence of advertised recruitment and a claimed process, without a confirmed victim or loss total. Housing and student-service communications should make independent verification routes clear [S1].

8.4 Mobile fraud includes more than card checkout

CERT Polska's September analysis linked 852 of 1,235 observed advertisements to 17 applications through common code or infrastructure. The analysis describes a route to premium messaging and operator billing. Those counts are advertisements and applications, not victims or charges [S15].

This creates a different customer-protection question from card replacement. A mobile subscriber can need operator-billing review, application removal and account recovery. The appropriate response depends on the actual application and transaction evidence.

The FvncBot analysis provides another mobile route: a convincing financial-service theme followed by additional installation and accessibility permissions. Its observed branding does not establish an incident inside the impersonated financial institution [S16].

8.5 Business email and payment changes

Supplier and accounting incidents can expose details that make a false payment instruction appear normal. The critical control is independent authority for the change, using contact information established before the request. A second person approving the same unverified message may repeat the original error.

Test the workflow with a synthetic supplier asking for a changed account, an urgent executive request and a supposed support call. The expected outcome is a safe pause, independent confirmation and a clear record of who approved the action.

Where a mailbox is involved, preserve its sign-ins, sessions, rules and relevant messages. Where an endpoint is involved, coordinate containment with account and session remediation. The report does not assume that every fraudulent instruction began with malware or a mailbox incident.

8.6 Price language is not market value

The selected offers provide asking prices with different units [S1].

Card	Advertised item	Asking price	Boundary
B01	Server-access claim	USD 200	Access unverified; not a completed transaction
B08	Purported public-body mailbox service	USD 550	Inventory and mailbox control unverified
B10	Claimed marketplace file	USD 1,980	Quantity, provenance and sale unverified

An advertised price can concern access, a file, a subscription or a service performed for a buyer. Currency, volume, freshness and exclusivity can be claims. Prices should not be combined across those units or interpreted as realised revenue.

The same applies to claims about demand. Many repeated advertisements can come from one persistent advertiser. A buyer request establishes interest expressed in a post, without demonstrating a purchase or a new incident.

8.7 A practical fraud-response hand-off

Signal	First owner	Validation	Closure evidence
A current account or access offer	Identity and SOC	Match account status, sessions and previous remediation	A reasoned disposition and proportionate response
A changed payee instruction	Finance	Confirm with a previously known contact	Independent approval or rejected change
A suspicious mobile charge	Fraud and operator support	Establish the billing route and application context	Customer case disposition and relevant access remediation
A notice-themed support call	Customer support	End the call and use the established contact route	Safe reconnection without sharing a verification code
A patient or student identity claim	Privacy and service owner	Determine the relevant records and controller scope	Scoped advice and a documented notification decision

8.8 Official campaign observations across the year

CERT Polska monthly summaries provide campaign-level context beyond named-organisation incidents. The examples below are recurring warning patterns, not ten unique victim incidents.

Month	Reported pattern	Defender action
January	Police-impersonation demands [S61]	Verify the institution through a known channel
February	Delivery-payment phishing [S62]	Open the trusted service independently
March	Authority-themed document demands [S63]	Do not send identity documents to an unverified contact
April	SIM-update credential and code phishing [S64]	Validate the request with the operator
May	Tuition demands from accessed university mailboxes [S65]	Verify payment authority outside the message
June	Payment-confirmation malware attachments [S66]	Validate the sender and inspect through the security process
July	Parking-payment SMS phishing [S67]	Use the independently opened payment service
August	Messaging-account linked-device QR fraud [S68]	Review linked devices and reject unverified enrolment
September	Government-themed lures leading to false bank sign-in [S69]	Verify the service before entering credentials
October	Tax-themed attachments carrying remote-access malware [S70]	Escalate suspicious attachments without opening them

8.9 Campaign and enforcement context

CERT Polska's 3 April cifrat analysis describes an Android remote-access chain delivered through a purported hospitality-application update. The source could not reliably assign the malware to an existing family. The analysis supplies no Polish affected-organisation count [S82].

CBZC's 31 March report describes a bank and courier phishing investigation. The operation date does not establish the campaign's start or place every loss in 2026. The July paid-DDoS investigation likewise does not establish a verified victim or attack total; suspects are not treated as convicted [S84][S85].

A 13 November CBZC report describes an invoice-fraud enforcement operation conducted in Poland. The listed victim countries were elsewhere. This is relevant to payment-instruction verification, without becoming a count of Polish victim organisations or proof of a completed conviction [S83].

KEY TAKEAWAYS

01

Genuine details do not establish authority to change an account or payment.

02

Mobile billing and malicious applications require a broader response than card checks.

03

Treat advertisements and asking prices as claims, with explicit transaction units.

CHAPTER 09

Banking and finance deep dive

THIS CHAPTER ANSWERS

Which identity and fraud controls follow from the selected financial-domain observations?

10 of 30

selected financial domains had a credential listed for sale

9.1 Population and limits 82
9.2 Employees, customers and shared identities 83
9.3 Payment instructions can be accurate and still fraudulent 83
9.4 Mobile applications can move the fraud boundary 84
9.5 Recent payment-provider access 84
9.6 Joint ownership for financial resilience 85

CHAPTER 09

Banking and finance deep dive

IN SHORT

10 of 30 selected financial domains had a credential listed for sale when checked. The portfolio contains at least 80,757 device associations, including 304 employee associations. The issuer-matched subset has a separate scope. Autopay's recent notice confirms access while leaving copying unresolved. Validate current accounts and payment instructions, and run employee-access investigations alongside customer-fraud protection.

9.1 Population and limits

The financial portfolio contains 30 candidate domains, including banks, payment services and market infrastructure. It is not a list of every licensed bank or card issuer. Exposure associations do not measure account misuse across Poland [S2].

Measure	Result	Boundary
Financial domains	30	Selected candidates, not all regulated entities
Domains with current listings	10 / 30	A credential offer, not confirmed infrastructure access
Device associations	≥80,757	Includes employee associations; other ownership unestablished
Employee-device associations	304	Included in the total above
Historical credential records	54,584	Not unique people or active accounts
DMARC quarantine or reject	24 / 30	Policy request, not proof of complete enforcement
DMARC monitoring	6 / 30	Validate legitimate senders before changing policy
Successful TLS validation	30 / 30	The observed connection, not every endpoint
HSTS observed	24 / 25	Responding homepages only

The bank-issuer match covers 21 candidate domains from the configured bank list. The broader financial portfolio also includes non-bank financial services and market infrastructure. The matched subset is not a verified national issuer census [S2][S4].

Matched subset	Result
Candidate bank domains matched	21
Matched domains with current listings	8
Other-device associations	49,440
Employee-device associations	272
Top-three share of other-device associations	62.2%

The concentration percentage concerns device associations within the matched subset, not card theft, losses or confirmed bank intrusions. Other devices are outside the employee classification; customer ownership is plausible but unestablished. Historical credentials and current listings retain separate account-validity limits.

SCOPE OF THE CARD FIGURES

Card figures cover only payment cards appearing in clear text in the collected posts. Brandefense detects stolen cards through many other methods outside this report. These figures do not measure card theft, validity or fraud loss.

The retained posts contain 455 distinct Poland-associated cards across 413 posts: 76 issuer-associated and 379 country-only, disjoint groups [S4]. Card observations are not added to device or credential totals. No bank ranking or bank-specific card values are published.

9.2 Employees, customers and shared identities

A device associated with a financial domain could belong to a customer, employee, contractor or another user. A credential record could concern a retired account or a reused address. Those distinctions should determine the first validation step.

Employee-access validation asks whether an account is active, what privileges it has, which sessions exist and whether the relevant device is managed. Customer-fraud validation asks whether a transaction, recovery request or new payee is genuine. Neither track should wait for an unsupported assumption about device ownership.

Historical identity information can remain useful to an impostor after passwords change. A customer-service process should therefore distinguish knowledge of a person's details from authority to act. Use a previously established channel for sensitive changes and explain the reason clearly to the customer.

9.3 Payment instructions can be accurate and still fraudulent

Fakturownia's confirmed scope includes business context that could make an instruction persuasive. It separately states that bank login credentials and payment-card details were not stored. An invoice-data incident and a bank-password incident require different responses [S10].

For a proposed payee change, the finance team should verify the instruction with a known contact and record the result. The security team can investigate the relevant mailbox, account and supplier. A genuine invoice number should not bypass independent approval.

The same approach applies to urgent requests citing a public incident. An impostor may claim that a payment must be moved to a protected account or that a security code is needed for investigation. Staff should end the interaction and use an established contact route.

9.4 Mobile applications can move the fraud boundary

CERT Polska's FvncBot analysis describes a bank-themed application leading users to additional modules and accessibility permissions. It says the distribution mechanism was not identified at the time. The branding is a lure, not evidence of access to the bank's systems [S16].

The September toll-fraud analysis describes a different route involving malicious applications and mobile billing. A payment or charge can therefore occur outside conventional card checkout. Banks, operators and customer-support teams need a shared escalation path, without assuming the same actor operates both campaigns [S15].

For managed devices, review application installation and sensitive permission changes. For customers, make the instruction concrete: a bank-support interaction should not require an unverified security component. A support script should provide a safe way to contact the institution again.

9.5 Recent payment-provider access

Autopay's November notice creates a focused validation task. It confirms unauthorised infrastructure and payment-information access, while copying and misuse remain unconfirmed. It recommends transaction review and reporting unauthorised operations through the bank [S45].

Do not automatically replace every card or infer that every customer is affected. Use verified provider and bank instructions, account-specific evidence and the relevant incident process. A disruptive response should have an evidence owner and a recorded reason.

9.6 Joint ownership for financial resilience

Team	Decision	Completion evidence
Identity and SOC	Is an external credential signal linked to an active account or suspicious session?	Documented validation and a proportional response
Fraud and customer support	Is the customer or instruction genuine?	Independent verification and a safe contact route
Finance and procurement	Is a supplier payment change authorised?	Known-contact confirmation and payment approval
Operations and compliance	Is the incident reportable under the applicable financial process?	Service facts and a signed reporting decision [S28]
Infrastructure and business owner	Can the payment workflow recover independently?	A tested transaction path and business acceptance

KEY TAKEAWAYS

01

Keep employee-access and customer-fraud investigations in parallel.

02

Accurate payment context is insufficient authority for a sensitive change.

03

Keep issuer concentration within the matched subset and its device-association denominator.

CHAPTER 10

Regulatory and national response

10

THIS CHAPTER ANSWERS

Which duties should legal and security teams distinguish at the cut-off?

3 April 2027

implementation milestone for entities covered by the specified KSC transition

10.1 Keep the legal instruments separate 87

10.2 KSC: registration, implementation and audit are different milestones 87

10.3 GDPR: the supplier does not replace the controller 88

10.4 DORA: join service and security evidence 88

10.5 What CISOs should do now 89

CHAPTER 10

Regulatory and national response

IN SHORT

Poland's KSC amendment is in force, with different registration, implementation and audit milestones. GDPR duties continue to apply to personal-data incidents, including those at processors. Financial entities also need their DORA reporting process. One incident can trigger several assessments with different clocks. Confirm entity scope, preserve the awareness timeline and prepare initial notices before the next supplier incident.

10.1 Keep the legal instruments separate

The table identifies the decision each instrument requires. It is an operational summary, not legal advice or an organisation-specific applicability opinion.

Instrument	Scope	Timing	Operational decision
KSC amendment, published act 2026/252 [S25][S26]	Essential and important entities meeting the statutory criteria; sector and transition rules matter	In force 3 April 2026; initial registration milestone 3 October 2026; specified implementation milestone 3 April 2027	Establish status and registration evidence; allocate control and management responsibilities
GDPR, Articles 33–34 [S27]	Controllers and processors handling personal data	Controller notification without undue delay and, where feasible, within 72 hours of awareness, unless risk is unlikely	Record awareness, assess risk, notify the supervisory authority when required
GDPR processor duty [S27]	Processor becoming aware of a personal-data breach	Notify the controller without undue delay	Give the customer enough information to assess its own obligations
DORA [S28]	Financial entities within its scope, with its own exclusions and proportionality rules	Applicable from 17 January 2025	Classify ICT incidents and follow the financial reporting route

The GDPR authority clock does not automatically begin when a newspaper publishes an allegation. Equally, a controller should not wait for a supplier's final report if it already has sufficient certainty. Preserve the facts supporting the actual awareness decision.

10.2 KSC: registration, implementation and audit are different milestones

The Ministry's detailed timetable gives 7 May–3 October 2026 for self-registration by entities outside the official-entry process. It identifies 3 April 2027 for implementation and use of S46 by entities meeting the stated conditions at entry into force [S26].

For new essential entities that were not previously operators of essential services, the first audit milestone is 3 April 2028. Existing operators retain their audit cycle. The guidance therefore does not support a universal statement that every organisation may postpone its next audit until 2028.

The amendment introduces early warning and subsequent incident reporting, with sector-specific routing and provisions for trust-service providers. Legal teams should map those requirements to the entity's applicable transition and existing duties. A general implementation period is not a reason to suspend an established incident process [S25].

Penalty provisions also require their own transition analysis. Article 73 includes an essential-entity ceiling based on EUR 10 million or 2% of business revenue, whichever is higher. It also contains separate important-entity and serious-consequence provisions [S25].

The Ministry's timetable places the start of penalty provisions at 3 April 2028. That date does not defer GDPR or DORA obligations. Do not use a possible maximum penalty as an estimate of likely financial loss [S26][S27][S28].

10.3 GDPR: the supplier does not replace the controller

UODO's August MyDr guidance calls for an assessment of whether the affected processing concerns the particular controller. It reminds controllers of authority notification and, where high risk is likely, communication to affected people [S6].

GDPR Article 33 allows information in phases where it cannot be supplied together. A late notification needs reasons for delay. Article 34 includes exceptions to individual communication, including specified protective measures or subsequent measures removing the likely high risk [S27].

The practical preparation is an evidence pack: what happened, when awareness arose, categories and approximate numbers, likely consequences, mitigation and a contact point. Approximate figures must remain estimates. A count of database rows should not become a count of affected people.

10.4 DORA: join service and security evidence

KNF's DORA hub identifies the regulation and the implementing texts on incident classification, reporting, contracts and testing. This makes financial resilience a joint concern for security, operations, procurement and compliance [S28].

A bank needs to know whether a payment service remains available, whether an ICT incident meets reporting criteria and whether personal data are involved. These are related assessments with separate legal tests. A supplier's reassuring service message does not close all three.

Maintain one factual incident timeline and separate decision records for each reporting route. This reduces contradictory numbers and dates while preserving the distinction between legal obligations.

10.5 What CISOs should do now

Action	Owner	Completion evidence
Confirm KSC entity status, registration and applicable transition	Legal and executive sponsor	Signed applicability note and registration receipt, or documented reason for exclusion
Reconcile existing audit commitments with the new timetable	Assurance	Current audit calendar, with the legal basis for each date
Rehearse a processor incident before complete facts arrive	DPO and procurement	An initial risk decision, staged notice and supplier information request
Connect DORA and personal-data incident assessments	Financial compliance and incident response	One factual timeline with separate signed reporting decisions
Verify the correct national or sector response channel	Incident response	Tested contact list and an alternate route if the main platform is unavailable

Escalation should not depend on a single mailbox or a single administrator. The ePUAP incident shows why an organisation also needs to understand alternative communication channels and the evidence of timely submission [S31].

KEY TAKEAWAYS

01
Treat registration, control implementation and audit dates as separate obligations.

02
Preserve the controller's awareness and risk decisions during supplier incidents.

03
Reconcile cyber, privacy and financial reporting through one factual timeline.

CHAPTER 11

Outlook

11

THIS CHAPTER ANSWERS

Which judgements are supported, and what would change the response?

4

planning scenarios with explicit triggers

11.1 Key judgements 91
11.2 What would change the assessment 92
11.3 Conditional scenarios 92
11.4 Avoid false certainty at the cut-off 92

CHAPTER 11

Outlook

IN SHORT

Supplier-held data and identity abuse are the strongest practical themes in the verified disclosures. Ransomware listings support recovery planning but cannot predict which organisation will be affected. Recent public-service restrictions show that restoration can require several stages. Use conditional scenarios, assign an evidence owner, and change the response when service or account facts change.

11.1 Key judgements

Confidence attaches to the stated proposition. High confidence in a published notice does not establish every estimate within that notice.

Judgement	Confidence	Basis and limit	Decision
Shared software can distribute incident-assessment work across independent controllers	High	MyDr, FELG and Fakturownia notices describe this dependency; not every customer is necessarily affected [S5] [S8][S10]	Require customer-specific incident information and a named recipient
Accurate historical data can support persuasive impersonation	Medium	Disclosed data categories include identities, contacts and business context; later misuse is not demonstrated for every case [S5][S10]	Verify authority through a previously trusted channel
Ransomware remains a continuity planning concern	High for visibility, uncertain for future incidence	Ransompedia records 56 Polish listings; private and unpublished incidents are missing [S3]	Test recovery of an essential workflow with independent credentials
An actor announcement is insufficient for service-impact attribution	High	DDoS material and official recovery accounts describe different evidence; no general causal link is established [S30][S31]	Measure availability and preserve logs before naming a cause
Current credential listings require account-specific validation	High for the observed association	Exposure observations concern selected domains; ownership, freshness and access remain separate questions [S2]	Match current accounts, sessions and prior remediation before disruptive action

These judgements do not predict the frequency of attacks, the likelihood of state action or financial losses. The evidence does not provide the population and controls needed for those estimates.

11.2 What would change the assessment

A controller's account-specific confirmation would move a supplier allegation into a defined incident scope. The identity team would then determine the affected accounts, sessions and recovery channels. The privacy team would assess the information about people separately.

A newly published credential or access advertisement would justify validation. A match to an active account and suspicious session would justify escalation. An old password, inactive account or unrelated domain would lead to a different, documented disposition.

Provider logs showing sustained service degradation would change a DDoS claim from an announcement into an operational availability investigation. They would not automatically establish the announcing group's responsibility. Matching timing alone is weaker than technical evidence.

A vendor's revised fixed-version guidance would change the patch plan. The RouterOS example illustrates why administrators must check the current advisory, rather than assuming the first version listed remains the recommended destination [S20].

11.3 Conditional scenarios

These are planning assumptions. They are not forecasts of events or claims that any named organisation currently lacks a control.

Scenario	Trigger	First response	Completion evidence
A processor discloses access to customer records	The provider confirms that your tenant or practice is included	Preserve the notice; identify data categories, awareness time and affected processes	A controller-specific scope and signed reporting decisions
A convincing invoice change follows a data notice	A supplier requests a new payment destination, citing real invoice details	Suspend the change and call a previously known contact	Independent confirmation and a logged payment decision
A public service restricts access after an incident	Users cannot complete an essential electronic submission	Activate the agreed alternative and preserve submission evidence	Business acceptance that the workflow works through the alternative
A politically framed group claims your public site	A claim appears with a target list or availability screenshot	Confirm service health with the provider and activate mitigation if needed	Recorded service measurements and a fact-based public update

11.4 Avoid false certainty at the cut-off

The last days are not a completed month. Public disclosures can lag access by weeks, as the university chronology demonstrates. A later statement can update an earlier incident without creating another case [S41].

The same limits apply to comparisons. Poland's partial 2026 listing total and full-year 2025 total are different durations. Their difference is a visibility comparison, not a measured annual growth rate. Comparator totals also differ in economic size and disclosure behaviour [S3].

Comparison countries were selected as examples to provide context only; they do not imply a ranking or political assessment.

Treat the outlook as a decision framework that can be revised. Each team should know the fact that would move it from monitoring to investigation, from investigation to containment, and from restoration to business acceptance.

KEY TAKEAWAYS

01

Give each judgement an evidence boundary and a change signal.

02

Use supplier, identity and availability triggers to start specific actions.

03

Reassess after new confirmations without counting updates as new incidents.

CHAPTER 12

Action plan

12

THIS CHAPTER ANSWERS

Who should act over 30, 60 and 90 days, and what demonstrates completion?

90 days

to test identity, supplier and recovery decisions

12.1 The 30/60/90-day plan 95

12.2 What each role should own 97

12.3 A practical completion scorecard 98

12.4 How Brandefense can help 99

CHAPTER 12

Action plan

IN SHORT

Start with the dependencies that can expose records or stop essential work: identity, shared software, payments and recovery. Assign business as well as technical owners. Test controls with synthetic records and approved exercises. Close an action when the expected decision or service has been demonstrated, rather than when a policy has been written. Use the following plan to set evidence-based priorities.

12.1 The 30/60/90-day plan

The lanes connect each action to a trigger or verified case. Targets below are proposed management objectives, not measured performance at Polish organisations.

1Days 1–30

For every essential workflow, identify the identity provider, processor, support contact and recovery dependency

OWNER

Business operations and architecture

COMPLETION EVIDENCE

An approved dependency register with an accountable service owner

If a supplier notice names your account, preserve it and establish the account-specific data scope [S5][S8][S10]

OWNER

Procurement and DPO

COMPLETION EVIDENCE

A documented awareness decision, data categories and initial reporting assessment

Where credentials or access are advertised, check account status, freshness, sessions and previous remediation

OWNER

Identity operations and SOC

COMPLETION EVIDENCE

A disposition for each signal and escalation of corroborated unauthorised use

If invoice or contractor data may be exposed, require independent confirmation of payee changes [S10]

OWNER

Finance and fraud

COMPLETION EVIDENCE

A synthetic fraudulent request is stopped and a legitimate request is completed

For exposed edge products, reconcile versions with the current vendor and CERT advice [S20][S23]

OWNER

Infrastructure

COMPLETION EVIDENCE

Version evidence, approved exceptions and an owner for every overdue action

Confirm KSC registration and applicable implementation dates [S25][S26]

OWNER

Legal and executive sponsor

COMPLETION EVIDENCE

A signed applicability note and a funded plan for outstanding duties

2Days 31–60

Prioritise phishing-resistant MFA for privileged and high-impact accounts [S14]

OWNER

Identity and business owners

COMPLETION EVIDENCE

Coverage measured against an agreed account inventory and a tested recovery route

Review suspicious sign-ins, new mailbox rules, token grants and unusual bulk exports

OWNER

SOC and messaging

COMPLETION EVIDENCE

Approved test activity reaches the analyst with account and session context

Where mobile access supports payments, review sideloading, accessibility permissions and carrier billing [S15][S16]

OWNER

Endpoint and fraud teams

COMPLETION EVIDENCE

A controlled test is blocked or detected, with a safe customer-support script

Restore one essential service using protected backups and independent recovery credentials [S35]

OWNER

Infrastructure and service owner

COMPLETION EVIDENCE

Successful workflow, data-integrity checks and business sign-off

Rehearse a processor incident while important facts remain unknown [S6][S27]

OWNER

DPO, procurement and incident response

COMPLETION EVIDENCE

An initial notice, unresolved-question log and scheduled update

Exercise an unavailable public submission or customer portal [S31][S34]

OWNER
Operations and legal

COMPLETION EVIDENCE
A usable alternative, preserved deadlines and a tested communication channel

3Days 61–90

Run a joint DDoS and public-claim exercise, separating provider measurements from actor statements [S30]

OWNER
Network, communications and SOC

COMPLETION EVIDENCE
Mitigation activation, fact-based updates and retained service evidence

For industrial processes, verify restoration of field communications and remote administration [S18]

OWNER
OT engineering and operations

COMPLETION EVIDENCE
Safe process validation, approved configuration and independent recovery access

Test supplier escalation outside normal working hours

OWNER
Procurement and incident response

COMPLETION EVIDENCE
A named supplier responder provides a scoped update within the agreed contract period

Present remaining control and evidence gaps to leadership

OWNER
CISO and service owners

COMPLETION EVIDENCE
Accepted residual risks, named owners and scheduled completion dates

12.2 What each role should own

Board and executive sponsor. Approve the service priorities and residual risks. Ask which business transaction has been restored in a test, which supplier can identify affected records, and who may authorise a service restart.

CISO and incident response. Maintain a decision log connecting each external signal to its verification and response. Keep an allegation, an official disclosure and an internally observed event as separate records until evidence supports a relationship.

Identity and messaging. Review privileged access, recovery channels and active sessions together. A password change alone may leave other access paths valid. Prefer phishing-resistant methods for high-impact accounts and test support-assisted recovery.

SOC and intelligence. Preserve the first observation, public updates and relevant internal logs. Avoid closing a claim solely because the service currently works. Equally, do not treat a country tag, screenshot or reused dataset title as proof of an intrusion.

Infrastructure and OT. Maintain trustworthy configuration and recovery access. Compare the actual installed release with the current advisory, then verify the service after changes. In industrial environments, include field communications and safe process operation in acceptance.

Finance and fraud. Treat correct invoice, identity or medical details as context an impostor may already possess. Confirm unusual instructions through a channel established before the request. Give call centres a safe method to end a suspicious interaction and contact the customer again.

Legal, privacy and procurement. Determine the controller and processor roles before an incident. During response, keep awareness, risk and notification decisions explicit. Require useful staged information from suppliers and record why a legal reporting route does or does not apply.

12.3 A practical completion scorecard

The scorecard measures whether the organisation can make and demonstrate the required decisions. It does not claim that any single control eliminates an attack route.

Question	Proposed target	Evidence
Do essential workflows have accountable owners?	Every workflow in the approved essential-service inventory	Named owner and dependency record
Can identity signals receive a reasoned disposition?	Every signal accepted into the triage queue	Freshness, account, session and remediation checks
Can a processor incident start the right clock?	Every exercised scenario has a documented awareness decision	Timeline, risk assessment and reporting decision
Can high-impact users resist credential relay?	Phishing-resistant MFA coverage against the agreed account inventory	Method inventory and a controlled sign-in test
Can payments survive convincing impersonation?	Every tested payee change receives independent verification	Recorded callback and approved payment
Can recovery survive loss of production administration?	Each selected essential workflow completes a recovery exercise	Restore record, integrity checks and business acceptance

Number matching is not counted as phishing-resistant MFA in this scorecard. An interim improvement should be labelled as such. The June campaign explicitly describes theft of one-time authentication codes [S14].

12.4 How Brandefense can help

Use external threat intelligence to turn an advertisement or credential signal into a verification queue for the appropriate owner. Combine that queue with your own identity, endpoint, supplier and service evidence. The required output is a reasoned decision, not a larger alert total.

This report demonstrates that approach through redacted evidence cards, separate source populations and actions tied to a completion test. The exposure section adds current listings, device and credential associations, and a national Atlas headline for the selected portfolio. Validate those signals against owned accounts and services.

Discuss the monitoring and validation questions that matter for your organisation: Request a demo.

KEY TAKEAWAYS

01

Give each priority a business owner and observable completion evidence.

02

Test supplier notification, payment verification and independent recovery together.

03

Close actions with demonstrated decisions and working services.

APPENDICES

Appendices

A–D

THIS CHAPTER ANSWERS

Which populations, dates and confidence limits govern the report?

4

evidence types kept distinct throughout

Appendix A. Method and evidence boundaries 101

Appendix B. Evidence register 105

Appendix C. Sources 106

Appendix D. Glossary 110

Appendix A. Method and evidence boundaries

Comparison countries were selected as examples to provide context only; they do not imply a ranking or political assessment.

A.1 Research contract

This report concerns Poland, country code PL. The post-date window is 1 January–22 November 2026. Public sources and passive observations were read on 22 November. The recent-activity focus is 9–22 November. The final day and November are partial.

The intended readers are security leaders, SOC teams, identity and infrastructure owners, fraud teams, legal and procurement. The report supports decisions about supplier scope, account authority, notification, essential-service recovery and public communication.

Sources include retained dark-web posts collected by Odin by Brandefense, public ransomware listings, passive DNS and TLS observations, official notices, legal texts and public research. Source-specific scopes remain attached to their conclusions.

A.2 Posts and advertisements

The publication population contains 118,390 country-associated posts. The retained content contains 119,484 distinct posts, including 1,434 forum posts. These are different populations. The retained content is partial, and no national crime total is extrapolated from it [S1].

The content assessment in Chapter 4 concerns 43,320 potentially relevant posts within 118,387 retained country-associated posts. Categories overlap. It does not measure unique offers, sellers, transactions or incidents.

An advertisement can describe older information. A poster's claimed export date is not a verified intrusion date. Similar wording supports advertising continuity, without establishing file identity or a common operator. Linked files and offered access were not acquired or tested for these case studies.

A.3 Selected organisations and passive observations

The private candidate list contains 250 domains. Exposure observations cover 250; passive observations cover 241. Selection is purposive and candidate identity still requires validation. The results therefore describe domains associated with the list, rather than a representative national sample [S2].

DMARC results describe policy requests, not complete enforcement. DKIM and delegation-record observations do not establish full signing or DNSSEC validation. TLS and homepage results retain their own conclusive or responding denominators.

The national Atlas headline is 51 out of 100. Only this national rating is published. Sector tables contain signal counts. Exposure counts were read on 21 November 2026; additional source counts and passive checks on 22 November 2026.

Device and credential associations can include older records. Mention counts cover the preceding 365 days; lookalikes cover 30 days. Associations overlap across sources and domains. None of these measures establishes unique people, active credentials or an organisational intrusion [S2].

A.4 Ransomware listings

Ransompedia supplies a source snapshot for Poland and four regional peers. The window uses listing publication dates or the source's alternative date where publication is absent. It does not establish intrusion dates [S3].

Country and group labels are source assignments. A listing can repeat an organisation or concern a multinational relationship. This report does not independently confirm all country assignments, encryption outcomes or the uniqueness of victims.

The 2026 window and full 2025 are different durations. Comparator economies and disclosure practices differ. Their totals are visibility comparisons, not national risk rankings or measured annual growth rates.

A.5 Payment-card material

The figures cover only cards appearing in clear text in collected posts. Brandefense detects stolen cards through many other methods outside this report. The 455 distinct Poland-associated cards are not a national theft measure, a validity test or a loss figure [S4].

The public edition provides only pooled counts. It contains no card numbers, individual payment information or issuer ranking. The issuer-linked exposure view covers a selected bank subset; other financial-service candidates remain in the broader sector portfolio.

A.6 Vulnerability verification

Every CVE referenced in the report or its cited technical titles was checked in NVD. The table separates first fixes for a specific issue from broader current product guidance. Verify installed editions and channels before applying an update [S20][S21][S22][S23][S24][S52][S53].

CVE	Affected versions	Verified remediation
CVE-2026-67279 and CVE-2026-86060	RouterOS 6.0 before 6.49.21; 7.0 before 7.23.4; 7.24 before 7.24.2	NVD identifies first fixes 6.49.21, 7.23.4 and 7.24.2. CERT's broader guidance recommends stable 7.24.3, long-term 7.23.6 or RouterOS 6.49.21, or later appropriate releases
CVE-2026-87850	nVision versions below 18, per CERT Polska	Version 18; NVD also identifies that fixed version
CVE-2026-21509	Office 2016, 2019, Microsoft 365 Apps and LTSC 2021/2024 families listed in NVD	Microsoft gives Office 2016 build 16.0.5539.1001 and Office 2019 build 16.0.10417.20095. Microsoft 365 Apps, Office 2021 and later receive service-side protection requiring an application restart

The table is defensive version guidance, not an exploit description. A vulnerability notice does not establish exploitation at any selected Polish organisation. The report publishes no offensive instructions or working code.

A.7 Public incidents and campaigns

Public reporting was examined across the window, including official CERT Polska, CSIRT GOV/ABW, CSIRT MON, UODO, Ministry and police material. Coverage remains partial; absence from the report does not establish absence of an incident.

Official monthly summaries describe selected campaigns and can repeat the same theme. A notice's publication or modification date is not automatically its incident date. Historical events disclosed in 2026 remain historical context.

The public incident register uses generic roles except approved publicly confirmed and widely reported names. Source URLs that identify withheld organisations are not published. Detailed personal values, contacts and victim endpoints are not published.

A.8 Confidence and political neutrality

Observation means retained material or a recorded measurement. A criminal claim means the underlying assertion is unverified. An official account establishes what the source reports within its stated scope. Analyst interpretation connects those facts to a decision.

High confidence applies to a specific proposition, not every assertion by a named actor. A listing is not proof of encryption, historical credentials are not current access, and an association is not ownership. Unverified does not mean fabricated.

State attributions, political alignment and campaign labels remain the source's assessments. Language does not establish nationality or sponsorship. The authors take no position on governments, Russia, Belarus, Ukraine, elections, territory or international policy.

Appendix B. Evidence register

The post cards contain short redacted excerpts and separate the offer from what remains unestablished. Posting dates do not establish intrusion dates. The underlying source mapping is retained privately.

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

The seven offer dossiers A–F and U refer to B01–B06 and B12. B17 supports Case V; the official notice and the larger seller totals retain separate scopes. B07 is a campaign mention; B08–B11 and B13–B16 are supplementary observations. The fifteen official-notice-led cases G–T and V are separate dossier entries. Case V also compares the related advertisement.

Appendix C. Sources

Each external source below was read for its supporting passage. The verified-on date records that source check, not independent confirmation of every claim the source reports. Own-data entries refer to retained evidence and public aggregates, rather than an externally reproducible national census.

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. Verified on 22 November 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. Verified on 22 November 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. Verified on 22 November 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. Verified on 22 November 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. Verified on 22 November 2026.

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

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

S8: FELG Software, Security incident and updates. https://status.felg.cloud/incydent. Verified on 22 November 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. Verified on 22 November 2026.

S10: Fakturownia, Security incident, expanded notice. https://fakturownia.pl/incydent-eng. Verified on 22 November 2026.

S12: enel-med, Patient-data incident notice, 27 September. https://enel.pl/komunikat/. Verified on 22 November 2026.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

S49: MITRE ATT&CK, Valid Accounts. https://attack.mitre.org/techniques/T1078/. Verified on 22 November 2026.

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

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

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

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

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

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

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

S75: Energetyka24, Energy-sector organisation website interruption; statement quoted. https://energetyka24.com/ (article URL withheld). The organisation's statement was read within the article; a standalone primary notice was not available for verification. Verified on 22 November 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. Verified on 22 November 2026.

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

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

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

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

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

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

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

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

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

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

S89: Retail company, Mail-tool access notice and February update. Source URL withheld to protect the organisation. Verified on 22 November 2026.

Appendix D. Glossary

Term	Plain meaning
Controller / processor	The organisation deciding why and how personal data are used / one handling them on its instructions
Current credential listing	An offer involving credentials at the observation date; account validity still needs checking
DDoS	Traffic intended to make a service unavailable to legitimate users
DMARC	A domain's policy request for mail failing authentication alignment
SPF / DKIM	Sender-authorisation and message-signing mechanisms used in email authentication
DNSSEC delegation record	A parent-zone record linking a domain to signing keys; not proof that the whole chain validates
HSTS	A web policy instructing browsers to use encrypted connections
KSC / S46	Poland's national cybersecurity framework / its information and reporting system
KYC	Identity checks used when onboarding or verifying a customer
Phishing-resistant MFA	Authentication tied to the legitimate service so a false login page cannot reuse the approval
Stealer log / combolist	Information captured by credential-stealing malware / a collection of login and password pairs
Toll fraud / direct carrier billing	Abuse of paid mobile services / charging through a mobile operator
OT	Systems used to monitor or control physical processes
TLP:CLEAR	Shareable without TLP restrictions; other applicable duties still remain

About this report

Prepared by Odin by Brandefense. Version 1.0, 22 November 2026. The English master and Polish edition share numbers, evidence identifiers, sources and directives. The Polish edition was translated with AI; the English edition prevails where they differ.

The report is a source-bound assessment, not a complete census of Polish cyber incidents. Recommendations state what an organisation can validate or improve. They do not establish that any named organisation lacked the recommended control.

© 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