COUNTRY REPORT · BRANDEFENSE COUNTRY REPORT · BULGARIA 2026 · TLP:CLEAR · 84 MIN READ

Brandefense Bulgaria Cyber Threat Landscape Report 2026

Identity exposure, extortion listings and a years-long intrusion into state networks in a new euro-area member

BY
Odin by Brandefense

PUBLISHED
21 November 2026

READING TIME
84 min read

EDITION
Version 1.0 · Public Research Edition · TLP:CLEAR

RESEARCH WINDOW
1 January–18 November 2026

96 of 250
organisations had a credential listed for sale on the day of the check

1,757
distinct posts in the Bulgaria-tagged set that concern Bulgaria specifically

19
ransomware leak-site listings for Bulgaria in 2026 after review, naming 17 organisations

110 USD
median asking price for a bank or payment account in reviewed posts

CONTENTS

01 Executive summary
02 Bulgaria's digital and security context
04 What we see on the dark web
06 Hacktivism, DDoS and disruption claims
08 The fraud economy
10 Regulatory and national response
12 Action plan
B Appendix B. Evidence register
D Appendix D. Glossary
Report map
03 National exposure: 250 leading organisations
05 Targeting examples by sector
07 Threat actors
09 Banking and finance deep dive
11 Outlook
A Appendix A. Method
C Appendix C. Sources
About this report

CHAPTER 1

Executive summary

01

THIS CHAPTER ANSWERS

What happened in 2026, what matters most for Bulgarian organisations, and what should leaders decide first?

4

decisions for leaders, each tied to evidence in the chapters

INSIDE THIS CHAPTER

Four decisions for leaders | The year in numbers

IN SHORT

For the 250 leading Bulgarian organisations we assessed, the main measured exposure is identity: infected-device and credential associations, and credentials listed for sale. The most consequential reported intrusion was a five-year espionage operation inside state document-exchange networks, disclosed by the government. Ransomware groups listed 17 Bulgarian organisations, and sellers advertised insurance customer data. Act in this order: validate your credential listings, centralise mail and document-system logs, then rehearse an extortion listing.

This report combines three of Brandefense's own data sources with verified public reporting. **Brandefense Blackhole** supplied 14,289 posts tagged as concerning Bulgaria and a further 9,862 related posts. It also supplied infected-device and credential records for 250 selected organisations, and card material that appeared in clear text in posts. **Ransompedia** supplied ransomware leak-site listings for Bulgaria and four regional comparators. **Atlas** exposure ratings were computed for the 250 organisations. These are separate populations and are never added together.

The national Atlas headline for the 250 organisations is 50 out of 100, where 0 means no risk observed and higher values mean more exposure.

1. Identity exposure is widespread; credential listings come first. 218 of the 250 organisations have infected devices associated with their domains (301,070 in total, a lower bound), and 241 have historical credential records. Two consumer webmail providers hold 99.3% of the 76.7 million credential records, because their domains are users' mail addresses; the other 248 organisations hold 565,935. These are cumulative association counts, held on 21 November 2026 whatever their capture date. They can involve staff, students or customers, and whether any login still works requires validation. [S1][S3]

96 of 250 organisations had a credential listed for sale when checked. Treat a listing as a reason to validate accounts, not as proof of a breach: it does not say how many accounts or whose. [S4]

2. The government reports a five-year intrusion into state networks. In August the Ministry of Innovation and Digital Transformation disclosed unauthorised access to administrative networks. In November it said the access had run since 2021 through the infrastructure that institutions use to exchange documents. The minister put the volume at a minimum of 130 GB, more than 62 million pages. He said several international groups were believed involved, with no conclusive link to a state. Checks so far had found no exposure of citizens' personal data. Nothing in our dark-web data can be tied to it. [S22][S23][S24][S25]

3. Ransomware groups posted about as many Bulgarian listings as Romanian and Greek ones. After review, Ransompedia holds 19 Bulgarian listings dated 1 January–18 November 2026 (17 organisations), against 7 listings in all of 2025. Romania has 20 and Greece 19 in the same window. The listed organisations include a holding company and its insurance subsidiary, a trading company, a pharmacy chain and an internet services company. None had confirmed an incident by our cut-off as far as we found. [S6]

4. Insurance customer data with national personal numbers was the year's most significant data claim. Between 30 August and 16 September at least three offers advertised Bulgarian insurance customer data with national personal numbers (EGN), one claiming "2.2M+" records. The data protection authority confirmed breach notifications from three insurance companies in two groups, without confirming volumes, and one insurer denied any intrusion into its own systems. Whatever the origin, EGN, birth date and address should be treated as known to criminals. [S1][S32][S34]

5. Fraud uses official names; one election-day outage remains unexplained. Police and CERT Bulgaria reported SMS phishing in the name of the police, the transport ministry and couriers, and call centres running investment fraud. Police said three to four companies a week lose money to pay-ee-IBAN fraud. On the April election day two state websites were reported unreachable for hours while the ministry said its systems were working normally. Hacktivist claims against Bulgaria were few in our data and none was confirmed. `[S19][S41][S48][S51][S62]`

Four decisions for leaders

1. **Treat current credential listings as an incident trigger, not a statistic.** Route every current market listing tied to your domains to the identity team and record a disposition within 5 working days. Escalate to incident response if an active account without multi-factor authentication (MFA) is found. Arrange monitoring of credential listings and infected devices for your domains from day 1, through an internal team or a provider (§12.1).
2. **Centralise logs for mail, identity and document exchange, and hunt backwards.** By the ministry's account, the state-network intrusion stayed hidden for about five years and was found while a national monitoring system was being deployed (§7.2). Keep logs long enough to look back months, and alert on new administrator accounts and mail-administration sign-ins.
3. **Settle your NIS2 status and rehearse the 24-hour report.** The amended Cybersecurity Act requires an early warning within 24 hours of a significant incident, with fines of up to 10 million EUR or 2% of turnover (§10). Name the reporter now, and rehearse it together with a ransomware leak-site listing.
4. **Join identity, fraud and security operations around citizen data.** Insurance and identity-document offers do not reveal a breached system, but they power impersonation and account-recovery fraud. Test contact-detail, payee and loan processes against an attacker who knows EGN, birth date and address.

The year in numbers

19 / 17

Ransompedia ransomware listings for Bulgaria dated 1 Jan-18 Nov 2026, after review / organisations they name (7 listings in all of 2025)

WHAT IT IS NOT

Not confirmed breaches; unlisted and unpublished cases are invisible

14,289

Blackhole posts tagged as concerning Bulgaria, 1 Jan-18 Nov 2026

WHAT IT IS NOT

Not a count of attacks; most are multi-country advertising

1,757

distinct tagged posts in which Bulgaria is the subject

WHAT IT IS NOT

Not unique incidents; counts are an upper bound

>130 GB

documents the minister said were downloaded from state networks since 2021

WHAT IT IS NOT

Not attributed to a state; not citizens' personal data, according to checks so far

250

leading public and private organisations assessed with Brandefense Atlas

WHAT IT IS NOT

Not a random sample; not a national prevalence estimate

301,070

infected devices associated with those 250 domains (8,860 employee-classified, excluding two webmail providers); cumulative, all records held on 21 Nov 2026

WHAT IT IS NOT

Not 2026-only, not unique people, not verified current infections; a lower bound

565,935

historical credential records across the 248 domains other than the two consumer webmail providers (76.7 million including them)

WHAT IT IS NOT

Not 2026-only; not unique accounts or active passwords

96 of 250

organisations with a credential listed for sale at the time of the check

WHAT IT IS NOT

Not a count of accounts or of confirmed breaches

126

distinct Bulgaria-associated payment cards seen in clear text in collected dark-web posts (81 attributed to a named issuer, 45 labelled only as Bulgarian)

WHAT IT IS NOT

Not a fraud-loss figure; narrow scope (§8.2)

59%

of the 250 organisations enforcing DMARC (148)

WHAT IT IS NOT

Not a measure of phishing success or delivery security

Report map

Twelve chapters, five reader paths. Start with the row that matches your role; each chapter opens with the question it answers, and chapters 2-12 close with three takeaways.

Board and executives

What happened, how exposed are we, and what should we decide?

GO TO 1 3 12

CISO and security leads

Which exposures are ours, which actors matter, and which controls come first?

GO TO 3 7 9 10 12

SOC and threat intelligence

What did the actors post, how are they connected, and what did the state-network intrusion teach?

GO TO 4 6 7 12 App. A-B

Fraud and customer protection

How are Bulgarian identities, accounts and cards traded, and where do banks see it?

GO TO 4 5 8 9

Communications and legal

How do we speak about unverified claims, and what does the amended Cybersecurity Act require?

GO TO 6 10 12

01 **Executive summary**
What happened in 2026 and what leaders should decide first

02 **Context**
Which features of Bulgaria shape the threats

03 **National exposure**
How exposed 250 leading organisations are

04 **Dark web**
What criminals post about Bulgaria specifically

05 **Sectors**
Which sectors are named and what response each needs

06 **Hacktivism**
What was claimed, what was confirmed, how to prepare

07 **Threat actors**
Who the actors are, how they connect, what the official record says

08 **Fraud economy**
How identities and accounts are turned into money

09 **Banking**
Where banks' visible exposure sits

10 **Regulation**
What the NIS2 amendments require now

11 **Outlook**
What to plan for and what would change the plan

12 **Action plan**
Who does what in 90 days

CHAPTER 2

Bulgaria's digital and security context

THIS CHAPTER ANSWERS

Which features of Bulgaria shape the threats in this report, and which official statements set the frame for 2026?

89.8%

internet penetration, with 9.26 million cellular connections

INSIDE THIS CHAPTER

2.1 A connected population with a strong mobile habit
2.2 The euro changeover as a fraud lure
2.3 Elections and the protection of state systems
2.4 A years-long intrusion into state networks
2.5 A new ministry and a new cyber law

IN SHORT

Four features shape Bulgaria's 2026 threat picture. The euro changeover gave fraudsters a new lure. Two national elections put state websites under watch. The government disclosed a years-long intrusion into the networks through which state bodies exchange documents. A new ministry now leads digital government and cybersecurity. Plan for identity fraud and espionage at the same time: harden mail and document exchange, and warn customers at each fraud wave and before major changes.

2.1 A connected population with a strong mobile habit

Bulgaria had 6.66 million inhabitants and 5.98 million internet users in October 2026, a penetration of 89.8%. It had 9.26 million cellular connections (139% of the population) and 4.80 million social-media user identities [S14].

The criminal data we hold for Bulgaria is almost entirely Telegram traffic, and English and Russian dominate it (Chapter 4). Bulgaria usually appears as one country on a multi-country price list, next to Romania, Greece and the rest of the European Union. Bulgarian-language posts are a minority, and their count drops from June; the series is not comparable across mid-2026 (§4.2).

2.2 The euro changeover as a fraud lure

Bulgaria adopted the euro on 1 January 2026 at a fixed rate of 1.95583 lev per euro [S15][S16]. Before the changeover the Ministry of Interior warned citizens about calls and e-mails that pretend to come from banks, post offices or the police. Such messages ask for card details or PINs, the national broadcaster reported [S17]. In January the ministry's cybercrime unit reported a rise in fake-buyer scams against sellers on classified-ad sites, with phishing links that ask for card data and 3-D Secure codes [S40].

The changeover matters for defenders because every new price, account notice and payment form gives a phishing message a credible reason to exist. Chapter 8 shows that the fraud cases authorities reported in 2026 follow that pattern.

2.3 Elections and the protection of state systems

Bulgaria held a parliamentary election on 19 April 2026 and a presidential election (first round 25 October, runoff 1 November 2026). Official statements on cyber activity around both elections were brief. On 19 April the e-government ministry said in the afternoon that it saw no increased cyber activity against strategic sites and no denial-of-service attacks [S18]. Later that day News.bg, citing a national television channel, reported that the ministry's and the Council of Ministers' websites were unreachable after a cyberattack. The ministry said its systems were working normally, and the sites were back shortly after 19:00 [S19].

A caretaker deputy minister later said only limited cyberattacks were observed in the final hours of election day [S20]. Before the October vote the State Agency for National Security issued additional cybersecurity instructions to all strategic sites and set up an election-protection task force [S21]. We found no official report of a cyber incident on 25 October; the 1 November runoff was not checked separately, and the election-commission website could not be read (Appendix A.8). This report takes no position on either election.

2.4 A years-long intrusion into state networks

On 5 August 2026 the Ministry of Innovation and Digital Transformation reported unauthorised access to certain administrative networks that may have lasted for years. It found the access while deploying a new national cybersecurity system [S22]. On 18 November it said the state had cut off what it called the longest and largest known cyber-espionage operation against the Bulgarian administration [S23].

According to the ministry, the attackers had held unauthorised access since 2021 to the infrastructure through which state institutions exchange information. They moved between its components and collected sensitive information. Checks so far had not found any exposure of citizens' personal data [S23]. At a briefing the minister said at least 130 GB, or more than 62 million pages, had been downloaded. He said several international hacking groups were believed to be involved, and that there was no conclusive evidence linking them to a particular state [S24][S25]. Chapter 7 sets out what is and is not established.

2.5 A new ministry and a new cyber law

In May 2026 Parliament merged the Ministry of e-Government into the former Ministry of Innovation and Growth, creating the Ministry of Innovation and Digital Transformation [S26]. CERT Bulgaria remains the national computer security incident response team [S27]. In February the National Assembly adopted amendments to the Cybersecurity Act that transpose the EU NIS2 Directive [S28]. On 1 October the ministry announced that the European Commission had closed its infringement procedure against Bulgaria [S29]. Chapter 10 sets out what changed for organisations.

Official figures show sustained pressure, though they use different units and periods. The cybersecurity manager of the state IT company Information Services said 1,513 cyber incidents were recorded in Bulgaria in 2025, mainly denial of service, phishing, impersonation e-mails and infostealer infections [S30]. The State Agency for National Security registered about 450 incidents at strategic sites in 2025 and described the intensity of hacking attacks as steadily rising [S31]. The two counts cover different populations and should not be compared.

KEY TAKEAWAYS

01

The euro changeover gave fraudsters a new lure, and one election day brought a reported outage of two state websites whose cause remains open.

02

The government reports a five-year intrusion into state document-exchange networks, which the ministry says it found while deploying a national monitoring system.

03

A new ministry and the NIS2 amendments reset who supervises cybersecurity and how fast incidents must be reported.

CHAPTER 3

National exposure: 250 leading organisations

THIS CHAPTER ANSWERS

How exposed are the country's 250 leading public and private organisations when they are scored the way Brandefense Atlas scores a customer, and which signal should be triaged first?

96 of 250

organisations had a credential listed for sale on the day of the check

INSIDE THIS CHAPTER

3.1 Universe card | 3.2 The national Atlas rating and current listings by sector | 3.3 Devices and credentials | 3.4 Current credential listings: the first item to triage | 3.5 Lookalike domains, exposed documents and mentions | 3.6 Email and web hygiene

IN SHORT

We assessed 250 leading Bulgarian organisations using Brandefense Atlas exposure ratings. Almost nine in ten have infected devices associated with their domains, nearly all have historical credential records, and 96 had a credential listed for sale when we checked. Two consumer webmail providers hold 99% of the credential records, so we report totals with and without them. Three in five enforce DMARC. Triage current listings first, then employee devices.

3.1 Universe card

Item	Definition
Population	250 organisations: 117 state-owned or public, 133 private
By sector	62 government bodies, 31 banking and finance, 23 retail and holding groups, 23 education, 22 energy and utilities, 18 transport and logistics, 18 media and entertainment, 16 manufacturing and industry, 11 insurance, 11 hospitality and tourism, 9 telecom and internet services, 6 healthcare
Selection	Purposive: state bodies and national portals, banks and payment institutions, state-owned enterprises, market leaders. Selected for size or systemic role, not ranked by revenue; no published Bulgarian top-250 ranking was used
Unit	One verified primary domain per organisation. All 250 resolve in DNS (21 November 2026)
Measurements	Infected devices and employee devices, breach-database, stealer-log and combolist records, dark-chat and dark-web mentions, lookalike domains, exposed documents and current credential-market listings
Public checks	DNS, TLS and HTTP header checks
Date	Counts read 21 November 2026. Device, credential and listing counts are all records held on that date, regardless of capture date (cumulative, not 2026-only)
Periods	Mention counts cover 19 November 2025–18 November 2026; lookalike counts cover the last 30 days
Not unique people	One person can appear in several sources; one device can hold logins for several organisations
Not representative	Results describe this list. They are not national prevalence rates

3.2 The national Atlas rating and current listings by sector

Atlas rates each organisation from 0 (no risk observed) to 100; higher values mean more exposure. This report publishes only the national headline for the 250 organisations: 50 out of 100. By sector, it shows how many organisations carry each signal.

How to read Atlas ratings.

Term	Meaning
National headline	One Atlas figure for all 250 organisations: 50 out of 100
Current listing	A credential tied to the domain on sale at the time of the check

Devices and credentials are common in every sector; current listings are the first item to triage

Share of organisations in each sector with the signal. Current credential listings are shown in coral.

	Infected devices	Employee devices	Credential records	Current listing	Listing history	Lookalikes (30 days)	Exposed documents
Media and entertainment (18)	94%	78%	100%	89%	89%	94%	83%
Telecom and internet services (9)	100%	67%	100%	78%	78%	67%	67%
Retail and holdings (23)	100%	70%	100%	65%	65%	87%	48%
Hospitality and tourism (11)	73%	55%	100%	55%	55%	64%	45%
Education (23)	100%	100%	100%	48%	48%	83%	39%
Banking and finance (31)	90%	55%	97%	39%	39%	94%	23%
Insurance (11)	82%	55%	100%	36%	36%	82%	9%
Transport and logistics (18)	78%	56%	100%	33%	33%	78%	11%
Government (62)	82%	60%	94%	23%	21%	85%	26%
Energy and utilities (22)	95%	59%	100%	18%	18%	64%	14%
Healthcare (6)	83%	33%	83%	17%	17%	50%	0%
Manufacturing and industry (16)	62%	62%	81%	0%	0%	56%	19%

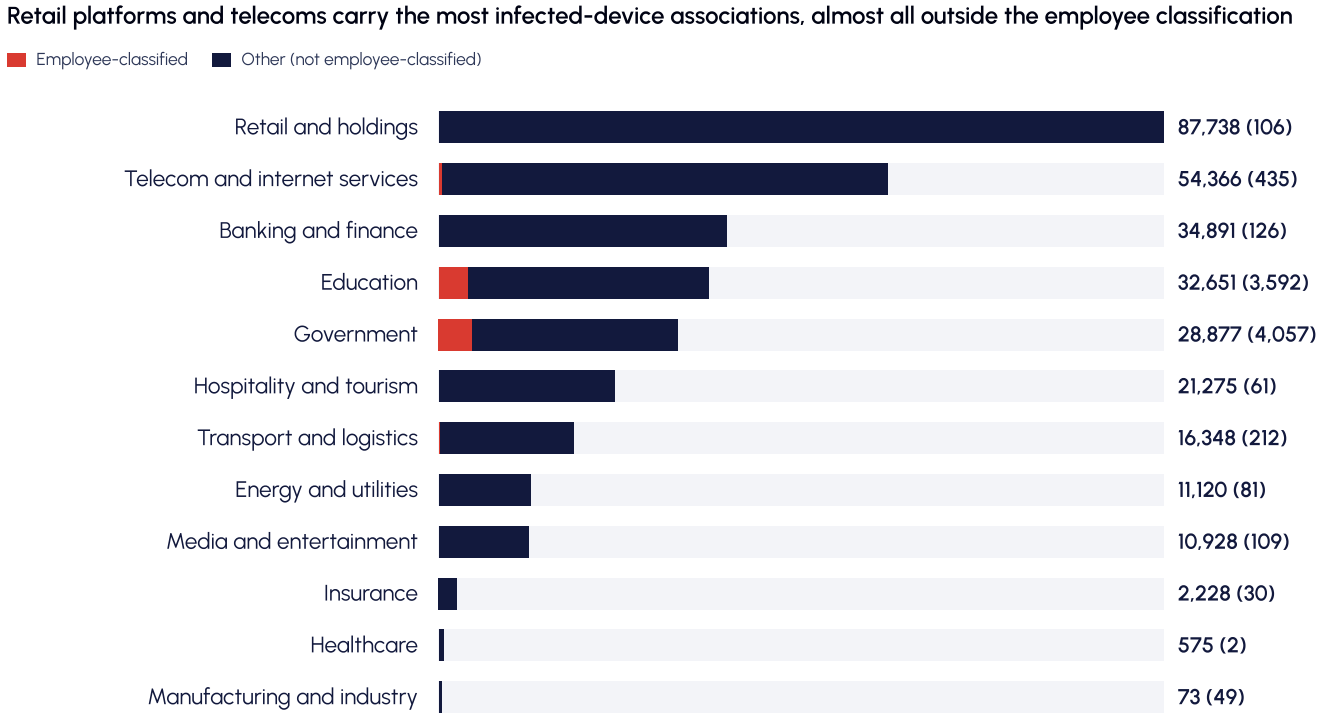
Source: Brandefense Blackhole associations and Atlas ratings for 250 organisations, read 21 November 2026 [S3][S4]. Records are cumulative, not 2026-only.

Sector	Orgs	Orgs with a current credential listing
Media and entertainment	18	16
Retail and holdings	23	15
Government	62	14
Banking and finance	31	12
Education	23	11
Telecom and internet services	9	7
Hospitality and tourism	11	6
Transport and logistics	18	6

Sector	Orgs	Orgs with a current credential listing
Energy and utilities	22	4
Insurance	11	4
Healthcare	6	1
Manufacturing and industry	16	0
All 250	250	96

Reading the table. A current listing is the first item to triage (§3.4); infected devices and credential records come next. We publish the Atlas rating as a national figure only.

3.3 Devices and credentials



Source: Brandefense Blackhole associations and Atlas ratings for 250 organisations, read 21 November 2026 [S3][S4]. Records are cumulative, not 2026-only.

Two organisations on the list run consumer webmail services. Their domains are the e-mail addresses of hundreds of thousands of private users, so almost every credential record and employee-classified device for those domains belongs to a user, not to staff. Together they hold 76.2 million of the 76.7 million credential records (99.3%). The table shows sector totals without them where they matter.

Sector	Orgs with infected devices	Devices (employee)	Credential records, excluding the
Retail and holdings	23 of 23	87,738 (106)	
Telecom and internet services	9 of 9	54,366 (435 without the webmail provider)	

Sector	Orgs with infected devices	Devices (employee)	Credential records, excluding the
Banking and finance	28 of 31	34,891 (126)	
Education	23 of 23	32,651 (3,592)	
Government	51 of 62	28,877 (4,057)	
Hospitality and tourism	8 of 11	21,275 (61)	
Transport and logistics	14 of 18	16,348 (212)	
Energy and utilities	21 of 22	11,120 (81)	
Media and entertainment	17 of 18	10,928 (109 without the webmail provider)	
Insurance	9 of 11	2,228 (30)	
Healthcare	5 of 6	575 (2)	
Manufacturing and industry	10 of 16	73 (49)	
All	**218 of 250**	**301,070 (employee-classified: 8,860, excluding the two webmail providers)**	

Device counts are lower bounds. Without the two webmail providers, credential records split into 69,075 breach-database records, 220,616 stealer-log lines and 276,244 combolist entries. The infected devices hold about 2.96 million captured credentials in total, for all services, not only the organisation's own.

What this means.

- **Consumer platforms carry the device load, almost all outside the employee classification.** Retail and classified-ad platforms, telecoms and banks have the most device associations. Their stealer logs include a login to the organisation's site, so they are most plausibly customers' own computers, though ownership is not established. These associations are a fraud and account-hijacking signal and do not by themselves establish an intrusion.
- **Government and universities hold the employee-device problem.** Government bodies have 4,057 employee-classified devices and education 3,592. Some government domains issue accounts to the public or to pupils and teachers, so "employee" may include non-staff users. The risk is credential reuse into systems that the same people access.
- **Concentration varies.** In government, two organisations hold 93% of the sector's credential records; in energy, the two largest hold 26%. A sector total is a poor guide to a typical organisation.
- **The median organisation is modest.** The median organisation has 70 infected devices and 391 credential records. The heaviest single organisations carry tens of thousands of devices or hundreds of thousands of credential records.

3.4 Current credential listings: the first item to triage

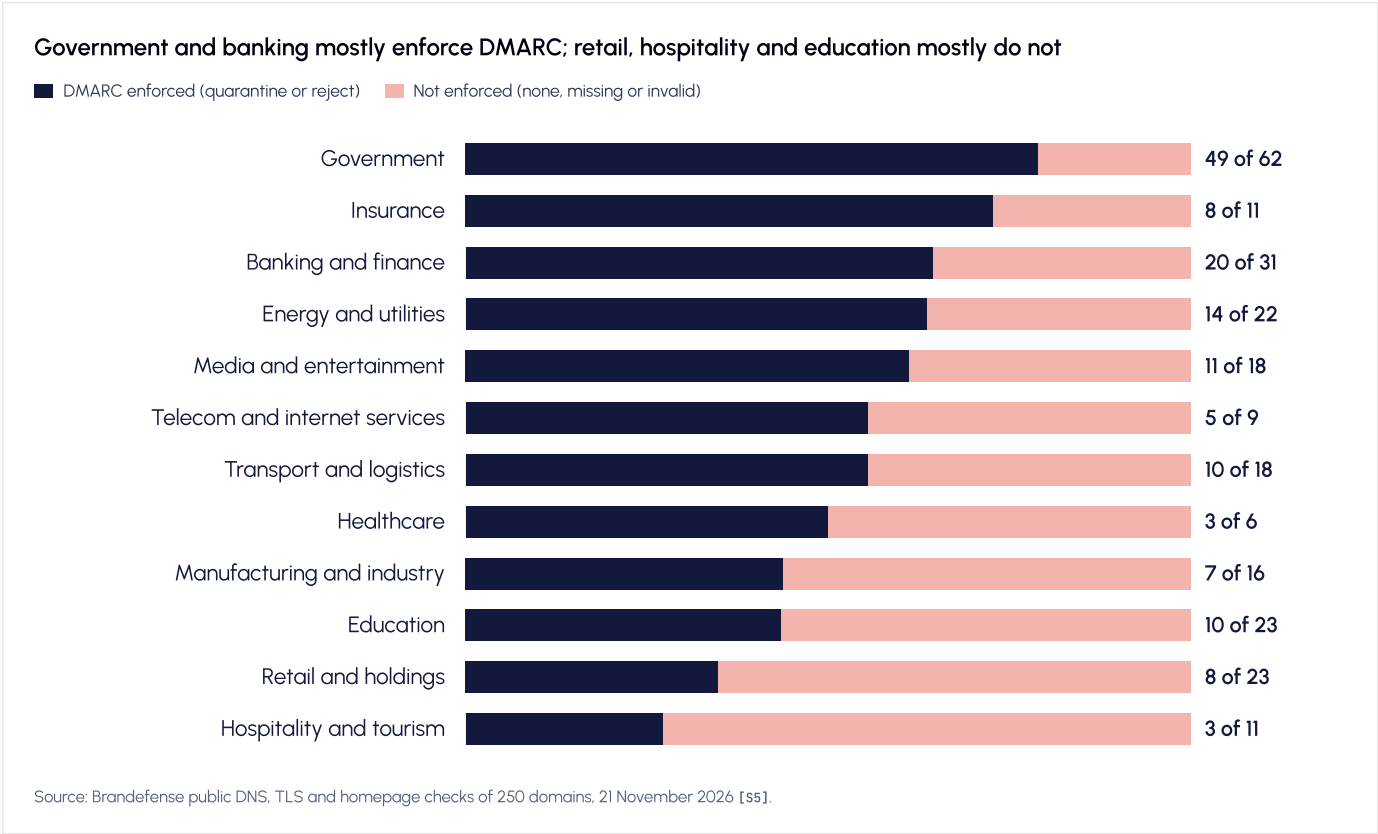
96 of 250 organisations had at least one credential tied to their domain listed on a monitored credential market at the time of the check.

For a defender, a current listing is the most direct market signal that a login tied to the domain is on offer. Whether that login still works is exactly what validation must establish. The listing does not say how many accounts, whose accounts, or whether the account is active, protected by multi-factor authentication, or already reset. The decision it supports is "validate the account now", not "declare a breach".

3.5 Lookalike domains, exposed documents and mentions

- **Lookalikes:** 200 organisations had at least one newly observed lookalike domain in the last 30 days. Lookalike coverage is incomplete for some organisations, and lookalikes are candidates, not confirmed phishing sites.
- **Exposed documents:** 78 organisations have at least one exposed document that references their domain (761 in total).
- **Mentions:** 55 organisations were mentioned in dark-chat sources in the last 365 days and 35 in dark-web (onion) sources. The largest counts belong to the consumer webmail providers, because their domains appear in credential lists. Mention counts measure visibility, not hostility.

3.6 Email and web hygiene



Source: Brandefense public DNS, TLS and homepage checks of 250 domains, 21 November 2026 [S5].

Email, DNS and web hygiene results [S5]:

Control	Result (of 250 unless stated)	Reading
DMARC reject	69	Spoofed mail from the domain should be refused
DMARC quarantine	79	Spoofed mail should go to spam
DMARC p=none or missing	102 (60 none, 42 missing)	No enforcement; spoofing the domain is easier
SPF ending -all / ~all / ?all / other / none	160 / 73 / 2 / 5 / 10	10 domains publish no SPF policy
DKIM found	163	Absence is not proof of no DKIM

Control	Result (of 250 unless stated)	Reading
DS record observed (DNSSEC delegation)	51	No DS record observed for 199 domains; a DS record alone does not prove a valid chain of trust
TLS certificate invalid	11 of 238 checked	Expired, mismatched or untrusted certificates
HSTS on homepage	110 of 197 reachable	Many sites do not force HTTPS for returning visitors
Mail provider	57 Microsoft 365, 28 Google, 8 no MX	The rest run their own or regional mail

Web checks could not be completed for 53 sites. Their DNS checks are complete.

Government leads on DMARC and DNSSEC; retail and hospitality lag. Of 62 government bodies, 49 enforce DMARC, and government domains account for 29 of the 51 with a DS record. In banking and finance, 20 of 31 organisations enforce DMARC. Retail (8 of 23), hospitality (3 of 11) and education (10 of 23) enforce least. On the passive hygiene index (Appendix A.5; 0-100, higher is weaker), hospitality (50), transport (48), education and manufacturing (47 each) have the weakest index values per sector, and government (35) and media (36) the strongest.

KEY TAKEAWAYS

01
Device and credential associations are widespread in the list; they call for validation, not alarm.

02
A current credential listing is the most direct market signal, so it is the first item to triage.

03
Two in five domains do not enforce DMARC, and only 51 of 250 publish DNSSEC delegation.

CHAPTER 4

What we see on the dark web

04

THIS CHAPTER ANSWERS

What do criminals post about Bulgaria specifically, and which offers matter to defenders?

1,757

distinct posts in the Bulgaria-tagged set that concern Bulgaria specifically

INSIDE THIS CHAPTER

4.1 Universe card | 4.2 Platforms, languages and volume | 4.3 Crime families after review | 4.4 Insurance customer data: the year's most significant data claims | 4.5 Government-themed claims | 4.6 Case studies | 4.7 What the forums add

IN SHORT

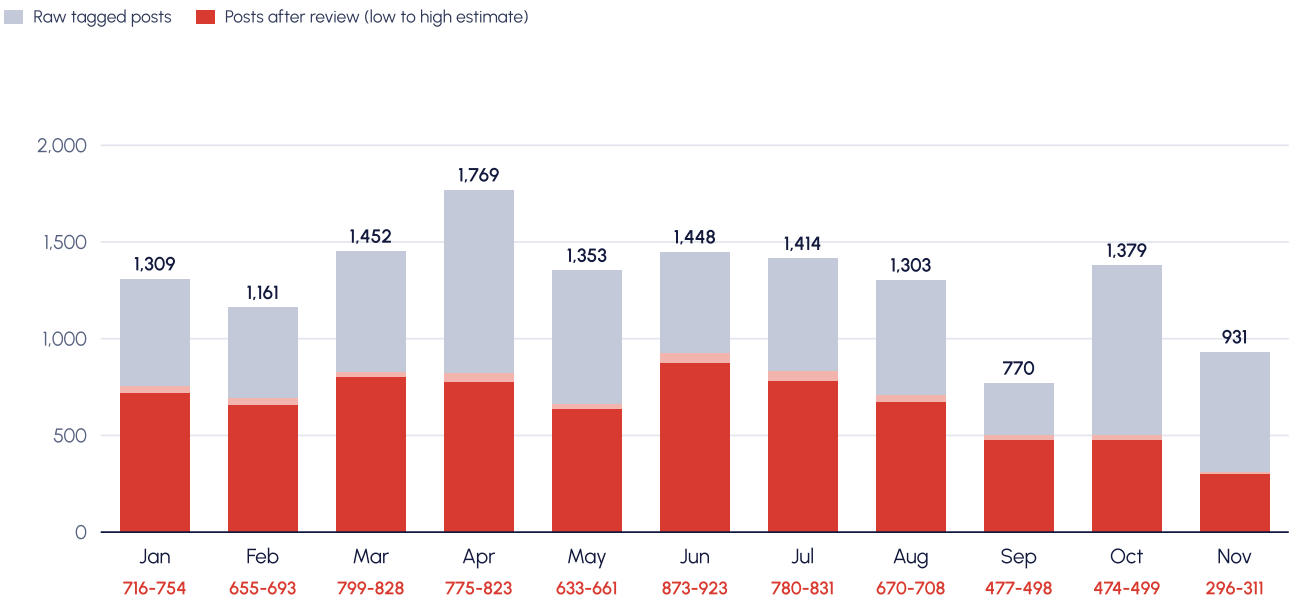
Most Bulgaria-tagged underground traffic is English and Russian Telegram advertising in which Bulgaria is one country among many. A smaller set concerns Bulgaria specifically: bank and payment accounts, identity documents, card-checker output, recurring "Bulgaria" combolists and webmail credential lists. The most serious 2026 offers claimed insurance customer data and government-related access. Read Bulgaria-specific counts, not raw volume, and triage each claim by provenance before comment.

4.1 Universe card

Item	Definition
Source	Brandefense Blackhole: Telegram channels and groups, a set of cybercrime forums, paste sites and Discord
Country definition	Posts tagged as being about, targeting or mentioning Bulgaria
Window	Post time 1 January–18 November 2026 (November partial)
Tagged set	14,289 posts counted; 14,286 distinct
Combined corpus	24,148 distinct posts: the tagged set plus 9,862 related posts
Tagged set after review	7,148–7,529 posts
Bulgaria-specific set	1,757 distinct tagged posts (3,325 in the combined corpus) in which Bulgaria is the subject rather than one entry on a multi-country list
Not established	That a tagged post targets Bulgaria, that a claim is true, or that two posts concern the same file

4.2 Platforms, languages and volume

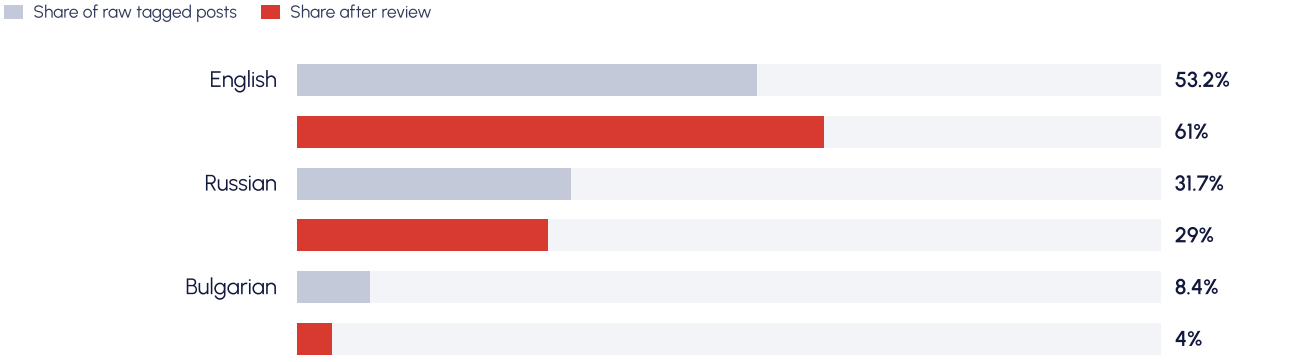
Bulgaria-tagged volume stays between 770 and 1,769 posts a month, without the template spikes seen in Romania and Greece



Source: Brandefense Blackhole, posts tagged as concerning Bulgaria, post dates 1 January–18 November 2026, November partial [S1]. Counts after review are an upper bound.

Measure	Value
Telegram share of tagged posts	98.6% (14,085)
Forum posts	165 (plus 305 related forum posts)
Paste, Discord, onion sites	27, 12, 0
English / Russian / Bulgarian / Turkish	53.2% / 31.7% / 8.4% / 1.7% of raw posts
After review: English / Russian / Bulgarian	61% / 29% / 4%
Raw posts per month	770–1,769 in complete months; 931 in the partial November window

English and Russian carry the Bulgaria tag; Bulgarian-language posts are a small share

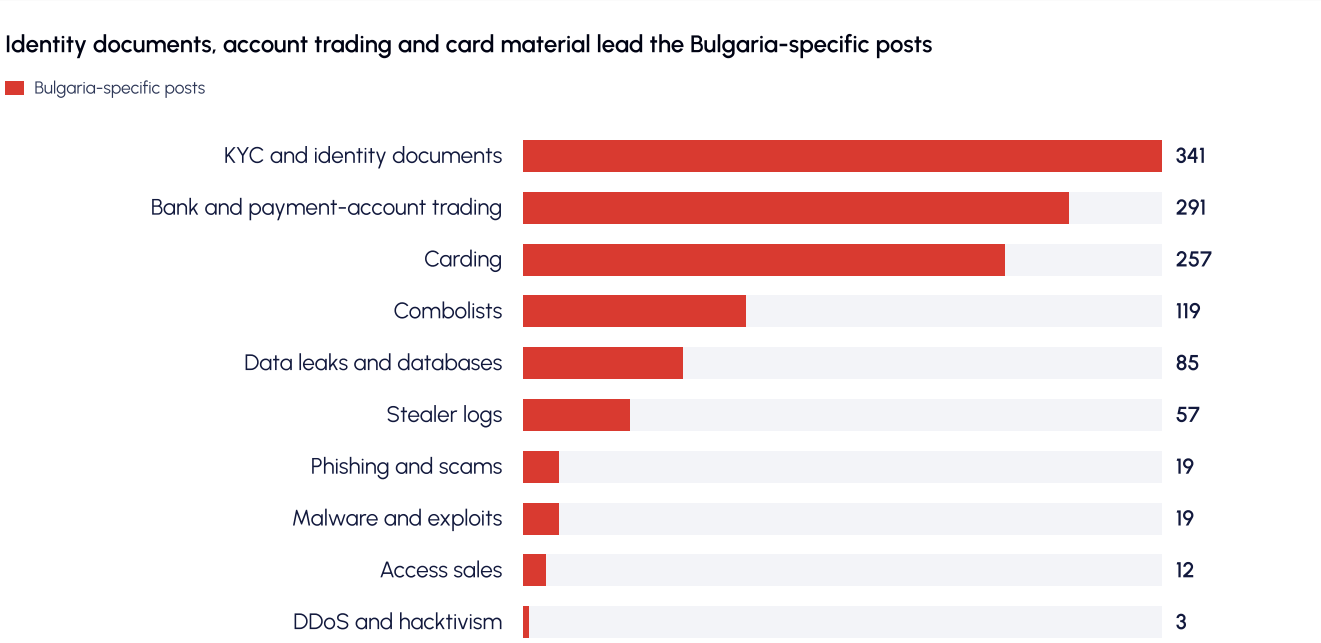


Telegram carries 98.6% of tagged posts. Language labels can overlap. Source: Brandefense Blackhole, posts tagged as concerning Bulgaria, post dates 1 January–18 November 2026, November partial [S1]. Counts after review are an upper bound.

Bulgaria shows no template spike. Romania and Greece each have more than 300,000 tagged posts in both January and February, driven by bulk multi-country advertising; Bulgaria's tag holds 1,161-1,309 posts in those months. After review, 474-923 posts remain in each complete month (January-October); the partial November window holds 296-311.

The series breaks in mid-year. Posts tagged as Bulgarian-language fall from 283 in May to 38 in June and stay below 10 a month afterwards. The monthly series are not comparable across mid-2026, so we do not read changes from June onwards as threat trends.

4.3 Crime families after review



Source: Brandefense Blackhole, posts tagged as concerning Bulgaria, post dates 1 January-18 November 2026, November partial [S1]. Counts after review are an upper bound.

Family	Posts after review (low-high)	Bulgaria-specific posts	What it contains
Data leaks and databases	2,842-2,890	85	Mostly two multi-country templates: card-shop stock updates and "physical persons" lead bases; Bulgaria-specific offers are far fewer
Bank and payment-account trading	2,040-2,151	291	Buying, renting and selling Bulgarian bank, fintech and payment accounts with Bulgarian IBANs
Carding	1,771-1,808	257	Card-checker outputs, card-shop updates listing Bulgaria, buyers of Bulgarian cards
KYC (know-your-customer) and identity documents	1,567-1,672	341	Verified accounts, ID-card and selfie sets, document templates
Phishing and scams	330-349	19	SMS-sending software, scam pages, "traffic" for scams
Combolists	208-228	119	Country-labelled "Bulgaria" credential lists and webmail credential lists
Malware and exploits	188-197	19	Tool sales and exploit discussion, mostly global
Access sales	152-181	12	Admin panels, website admin accounts, remote servers
Stealer logs	133-147	57	Log sales, "cracked and inboxed" account lists (password cracked, mailbox access checked)

Family	Posts after review (low-high)	Bulgaria-specific posts	What it contains
Ransomware (relays)	21	21	Relays of leak-site claims (Chapter 7)
DDoS and hacktivism	11	3	Small; see Chapter 6

Families overlap and must not be added. The ransomware row counts relays in the tagged set and is not part of chart c02. Two repeating multi-country templates inflate the reviewed data-leak and carding families. One card shop posted 1,073 stock updates that list Bulgaria among dozens of countries, and a lead-base advertisement was reposted more than 1,200 times. The Bulgaria-specific column is the better guide to what concerns Bulgarian organisations.

Prices quoted. In reviewed posts that quote a price, the median asking price was 110 USD for a bank or payment account and 100 USD for KYC and document services. Access offers had a median of 400 USD (few values) and combolists 50 USD. Named single Bulgarian offers ranged from 10 USD for a claimed government mail panel to 250 USD for a ready account at a Bulgarian bank (Chapter 8); the medians above include multi-country posts. These are asking prices, not completed sales.

4.4 Insurance customer data: the year's most significant data claims

Between late August and mid-September 2026 several venues advertised customer data attributed to Bulgarian insurers. None was independently verified, and we did not obtain any file.

Date	Claimed dataset	Claimed fields	Claimed volume	Venue	Post
30 Aug	"Bulgarian insurance company customer database", described as derived from national identity-number records	Customer ID, ID type, name, gender, birth date, address, phone, e-mail	"2.2M+" records, year 2025	Lead-trading Telegram channel	B01
10 and 16 Sep	"Bulgaria insurance database" with a sample header	Person ID, ID type (national personal number), names in Cyrillic and Latin, sex, birth date, region, city, address, phone, e-mail	Not stated	Cybercrime forum, sale via Telegram	B02
1 Sep (reported 10 Sep)	Records attributed to a large insurer, reported by press relaying a forum post; the seller blamed a weakly protected customer-portal API	National ID and passport numbers, addresses, contacts	3,134,269 rows	Forum (press report)	None [S32]
Sep (reported 26 Sep)	Records linked to a second insurer, reported by an investigative outlet and relayed by a security news site	Names, personal numbers, addresses, phone numbers	"More than 300,000"	Not stated	None [S34]

What is officially confirmed. The data protection authority (CPDP) replied to a public-information request on 24 September. It confirmed personal-data breach notifications from two insurance companies of one group on 3 August and from a second insurer on 11 September, and said it had opened proceedings [S34]. It did not confirm the number of records. One of the insurers denied any intrusion into its own information systems, according to the same report [S34].

What this tells defenders. The posts do not show which system the data came from, and the fields overlap with what many organisations hold. Whatever the origin, the advertised fields include the national personal number (EGN), birth date, address and phone. Banks, telecoms and insurers that verify callers with those fields should assume they are known to criminals.

EVIDENCE CARD B01 — 30 Aug 2026

Lead-trading channel Lead-trading Telegram channel · Telegram · English

ORIGINAL

```
Bulgarian Insurance Company Customer Database — 2.2M+
Records 🇧🇬
A structured database containing approximately 2.2M+
customer records associated with a Bulgarian insurance
company.
Source: Bulgarian insurance customer database (EGN/[state-
register]-derived).
Year: 2025
Data fields: Customer ID, ID type, customer type, name,
gender, birth date, country, region, city, address, postal
code, phone, and email.
DM on Telegram: [contact removed]
```

Note. EGN is the Bulgarian personal identification number. The poster's description of the source is its own claim.

HELD	The offer, the claimed fields, the claimed year and the claimed volume.
NOT ESTABLISHED	Which insurer, whether the data came from an insurer at all, any link to state registers, any sale.

EVIDENCE CARD B02 — 10 Sep 2026

lauraallen Cybercrime forum · Forum

· English, sample header in Latin script, sample rows in Bulgarian

ORIGINAL

```
Bulgaria Insurance Database
For Order DM on Telegram: [contact removed]
Code: PERSON_ID ID_TYPE PERSON_TYPE MAN_ID NAME GNAME SNAME
FNAME SEX BIRTH_DATE NAME_ENG ADDRESS_TYPE COUNTRY_ID
COUNTRY_NAME STATE_ID STATE_NAME REGION_ID REGION_NAME
CITY_ID CITY_NAME ADDRESS POST_CODE PHONE E_MAIL
[sample rows with names, personal numbers and addresses
removed]
```

Note. The sample rows carry the ID type "EGN". The same post was repeated on 16 September.

HELD	The offer, the field structure and that sample rows were posted.
NOT ESTABLISHED	Which insurer, whether the sample is genuine, file size, any sale.

4.5 Government-themed claims

Date	Observed post	Our reading	Post
5 Apr	A forum seller offers a "Bulgarian eGov mail admin panel" for 10 USD, claiming it can create unlimited government mail accounts on five domains, alongside panels for other countries	Unverified access claim; the low price and multi-country list suggest a reseller of stolen mail-account logins, not proof of a panel breach	B04
10-11 Aug	A forum thread titled "[BG] Bulgaria Starred Bears" claims to expose data from Bulgarian systems, with screenshots described as reconnaissance, foothold, Linux pivoting and database work; relayed by a hacker-news channel	Unverified; relayed five to six days after the government's first disclosure of a years-long intrusion (§2.4); no shared element links the two	B03
11 Aug	An automated forum uploader posts a small file of e-mail and password lines for a ministry's mail domain	Consistent with stealer-log or reuse lines from users' own devices (an inference); no evidence of a mail-server breach	None
22 Aug	A group calling itself Enigma Group posts what it says are backend VPN and network addresses of a state transport-sector system, taken from an administrator's uptime checker	Unverified; if genuine, it is reconnaissance data, not proof of access	B12

What this tells defenders. Government-themed posts in 2026 are about mailboxes and access, not population databases. A cheap "panel" or a file of a few lines for a ministry domain usually means stolen user logins. That still matters: in July CERT Bulgaria reported bomb-threat e-mails sent to state institutions from hijacked accounts that passed SPF, DKIM and DMARC checks [S35]. Mail authentication cannot stop a message sent from a real mailbox that someone else controls.

EVIDENCE CARD B04 — 5 Apr 2026

DuperKinger123 Cybercrime forum · Forum · English

ORIGINAL

```
Bulgarian eGov mail admin panel - 10$ (Can create infinite
gov mail accounts on 5 different domains)
[offers for other countries' government mail panels and
mailboxes omitted]
If your looking to buy any of these or have any questions dm
me on tele [contact removed]
```

HELD	The offer and the price.
NOT ESTABLISHED	Which platform, whether the panel exists, any account created, any sale.

EVIDENCE CARD B03 — 11 Aug 2026

Relay channel Hacker-news Telegram channel relaying a forum thread · Telegram · English

ORIGINAL

```
BULGARIA: Threat Actor Publishes Alleged Government-Related
Data
A threat actor has posted material under the title "[BG]
Bulgaria Starred Bears," claiming to expose data associated
with Bulgarian systems.
* The post contains multiple alleged proof-of-compromise
artifacts.
* Files shown include references to reconnaissance, foothold
access, Linux pivoting, database cross-referencing, and an
SSRF/proxy handler.
* [...] the specific claims remain unverified.
```

Note. The thread itself was not reviewed for this report.

HELD	That a thread with this title was posted and relayed, and how the relay described it.
NOT ESTABLISHED	Any intrusion, any data, the actor, any link to the intrusion the government disclosed on 5 August.

EVIDENCE CARD B12 — 22 Aug 2026

Enigma Group Leak forum · Forum · English

ORIGINAL

```
Hello, we are Enigma Group, and today we've decided to leak
the [a state transport-sector system] BACKEND IPs. This leak
contains IPs of VPN servers, WANs [...] All this info is
taken from admin's uptime checker.
```

HELD	The claim and its stated source.
NOT ESTABLISHED	Whether the addresses are genuine or current; any access to the system.

4.6 Case studies

Each case follows the same structure: claim, chronology, what we can establish, alternatives, limits and a proportionate response.

A

CASE A

Several offers of insurance customer data within three weeks

Evidence card B01 | 30 Aug 2026 | Lead-trading Telegram channel | Insurance

CLAIMS UNVERIFIED; NOTIFICATIONS FROM THREE INSURERS IN TWO GROUPS CONFIRMED

Claim	A lead-trading channel offered "2.2M+" records of a Bulgarian insurer's customers on 30 August. A forum seller posted a "Bulgaria insurance database" sample on 10 and 16 September.
Chronology	The regulator received breach notifications from two companies of one insurance group on 3 August and from a second insurer on 11 September [S34]. On 10 September press reported a forum offer naming one insurer, first observed on 1 September [S32]. An investigative outlet later reported more than 3 million records linked to one insurer and more than 300,000 to the other [S34].
What we can establish	That at least three offers of Bulgarian insurance customer data appeared between 30 August and 16 September, and that the regulator received notifications from three insurance companies in two groups. The posts do not establish which offer matches which notification, or that the files are identical.
Alternatives	One dataset resold under several titles; separate datasets from the two insurance groups; aggregated data from other sources relabelled as insurance data.
Response	Insurers and their brokers should compare any sample with their own export schemas and review partner and portal API access. Banks and telecoms should treat EGN, birth date and address as public when they verify callers.
BOTTOM LINE	**Treat EGN, birth date and address as known to criminals; insurers should compare any sample with their own exports before comment.**

B

CASE B

A "government data" claim days after an official disclosure

Evidence card B03 | 11 Aug 2026 | Hacker-news Telegram channel relaying a forum thread | Government

CLAIM UNVERIFIED

Claim	On 10-11 August relays reported that a forum thread titled "[BG] Bulgaria Starred Bears" claimed to expose data from Bulgarian systems, with screenshots the relay described as reconnaissance, foothold access, Linux pivoting and database cross-referencing.
Chronology	The ministry's first disclosure of years-long unauthorised access to administrative networks came on 5 August [S22]. The relays followed five to six days later. The ministry's fuller statement came on 18 November [S23].
What we can establish	That a forum actor made a government-themed claim with technical screenshots shortly after the disclosure. The thread itself was not reviewed for this report. No shared element links the post to the intrusion the ministry described.
Alternatives	An actor exploiting news coverage; an unrelated intrusion; genuine material from the disclosed intrusion.
Response	For government security teams, compare the screenshots, if obtained, with the incident's known indicators before any public comment.
BOTTOM LINE	**A forum claim after an official disclosure is not evidence about the disclosed intrusion; compare indicators before comment.**

C

CASE C

Government mailboxes are sold cheaply

OFFER OBSERVED (ONE POST)

Evidence card B04 | 5 Apr 2026 | Cybercrime forum | Government

Claim	On 5 April a forum seller offered a "Bulgarian eGov mail admin panel" for 10 USD, alongside government mail panels from other countries.
What we can establish	The offer and its price. A government-mail "panel" at that price is more consistent with a stolen user or administrator login than with control of a mail platform; the post does not show which.
Why it matters	It links to an official observation: in July CERT Bulgaria reported threat e-mails sent from hijacked accounts that passed mail authentication [S35].
Response	Government and municipal IT teams should review administrative sign-ins to mail platforms, enforce phishing-resistant MFA for mail administrators and alert on mass account creation.
BOTTOM LINE	**Treat a cheap government mail-panel offer as an unverified access offer; as a planning choice, review mail-administrator sign-ins and enforce phishing-resistant MFA.**

D

CASE D

Monthly "Bulgaria" combolists and webmail credential lists

RECURRING OFFERS

Evidence card B05 | 20 Apr 2026 | Cybercrime forum | All sectors

Claim	A seller brand posted a "Database: Bulgaria, Email:Password, FRESH" combolist at least six times between January and October, from 68,000 lines in January to 126,000 in April. A second brand posted similar lists of 56,000-150,000 lines.
Chronology	Separate posters advertised lists of "valid" accounts at a leading Bulgarian webmail service. One offered "1k valids ... able to be logged in and view emails" in February; another posted a "338X ... freshly cracked and inboxed" list in August. Several mail-checker tools advertised in October and November name the same service as supported.
What we can establish	A steady supply of Bulgaria-labelled credential lists and tooling to test them. The posts do not show the lists' origin, overlap or validity.
Alternatives	Repackaged old breach data; lists built from stealer logs; a mix.
Response	Organisations whose staff use personal webmail for work should block it for corporate sign-up, and should monitor for staff addresses in such lists. Webmail users need MFA.
BOTTOM LINE	**Expect Bulgarian credential lists every month; block personal webmail for work and require MFA.**

EVIDENCE CARD B05 — 20 Apr 2026

thejackal101 Cybercrime forum · Forum · English

ORIGINAL

```
Database: Bulgaria Type: Email : Password Date: [
20/APR/2026 ] Combo: [ 126 K++] Line Status: FRESH | HQ
Hidden Content You must reply to this thread to view this
content [...]
For more fresh Log's: [link removed]
```

Note. The same brand posted lists in this format at least six times between January and October.

HELD	The offer, the claimed size and the claimed freshness.
NOT ESTABLISHED	Origin, overlap with earlier lists, validity of any line.

EVIDENCE CARD B06 — 8 Aug 2026

kookiegst Cybercrime forum · Forum · English

ORIGINAL

```
338X [webmail service] BULGARIA FA HITS FRESHLY CRACKED AND
INBOXED PLEASE LEAVE A LIKE AND SUPPORT [...] NOTE : SOMEONE
ELSE CAN CLAIM THE ACCOUNT BEFORE YOU
```

Note. "Hits" and "inboxed" mean the poster says the passwords were tested and the mailboxes opened.

HELD	The claim of 338 tested mailboxes at a Bulgarian webmail service.
NOT ESTABLISHED	Any breach of the service; validity; whose mailboxes.

EVIDENCE CARD B07 — 16 Feb 2026

UHQCombos Cracking forum · Forum · English

ORIGINAL

```
I got 1k [webmail service] valids, might get 2k in total
soon, all able to be logged in and view emails etc, offer
price, DM me here or on Telegram [contact removed]
```

HELD	The offer.
NOT ESTABLISHED	Validity, origin, any sale.

E

CASE E

Retail and health-platform customer databases

CLAIMS UNVERIFIED

Evidence card B08 · 18 Feb 2026 · Breach forum · Retail and health

Claim	On 29 January a forum seller offered 32,683 records said to come from a health-care platform with Bulgarian users, breached two days earlier, for 50 USD. On 18 February a seller offered an online retailer's database of "around 4M records", sorted to 1.8 million lines. A breach-monitoring blog, relayed in our data, reported a furniture retailer's customer and order records offered for sale in February.
What we can establish	The offers, the claimed fields (names, e-mail, phone, city, birth date, gender or address) and the prices. None was verified, and none of these organisations had confirmed a breach by our cut-off as far as we found.
Alternatives	Older exports; scraped or aggregated data; genuine breaches.
Response	E-commerce companies should check for bulk exports and API abuse on the claimed dates and prepare customer warnings about order-themed phishing.
BOTTOM LINE	**Check bulk exports and API logs on the claimed dates; warn customers about order-themed phishing.**

EVIDENCE CARD B08 — 18 Feb 2026

Jurak Breach forum · Forum · English

ORIGINAL

```
[online retailer] is an online retail platform in Bulgaria
that offers consumer goods [...] The data contains around 4M
records, I've sorted it to around 1.8M unique lines (around
400k lines are missing names or phone numbers). name,
address, email, phone
Send a message with your offer
```

HELD	The offer, the claimed fields and counts.
NOT ESTABLISHED	Origin, age, any breach at the retailer, any sale.

EVIDENCE CARD B17 — 29 Jan 2026

temporary Breach forum · Forum · English, sample rows in Bulgarian

ORIGINAL

```
Hello, Breach Forums, I'm selling the database of [health-
care platform] [...] Total lines: 32.683 Breach date: 27-01-
2026 Price: $50 Fields: email, first name, last name, city,
date of birth, gender
Samples: [rows with names, e-mails, phone numbers and birth
dates removed]
```

HELD	The offer, the claimed fields, the claimed breach date and the price.
NOT ESTABLISHED	Any breach at the platform; that the sample is genuine; any sale.

F

CASE F

Access to infrastructure and devices is advertised

CLAIMS UNVERIFIED

Evidence card B16 | 23 Aug 2026 | Leak forum | Devices and infrastructure

Claim	On 23 August a forum poster offered addresses, user names and passwords for 140 cameras in Bulgaria, with snapshot links. In February a seller offered admin access to a Bulgarian events company's website for 50 EUR. In April a chat user said they had access to a Bulgarian bank's developer portal and asked whether it was worth selling.
What we can establish	The offers and claims. None was verified; the bank-portal claim is a single chat message without evidence.
Why it matters	Internet-exposed cameras and controllers are a recurring entry point. In November CERT Bulgaria warned of attacks across Europe on internet-exposed refrigeration controllers [S37], and Z-Pentest claimed control of a greenhouse control panel in Bulgaria (Chapter 6).
Response	Remove default credentials from cameras and controllers and take their management interfaces off the internet.
BOTTOM LINE	**Remove default credentials and take camera and controller management off the internet.**

EVIDENCE CARD B16 — 23 Aug 2026

updap (forum poster) Leak forum · Forum · English

ORIGINAL

```
140 cameras in Bulgaria IP:PORT,USER,PASS with snapshot
links
You have not unlocked this post's content yet. [...]
```

HELD	The claim of 140 camera logins.
NOT ESTABLISHED	Whose cameras, validity, any access.

EVIDENCE CARD B09 — 23 Feb 2026

Commando Breach forum · Forum · English

ORIGINAL

```
Selling Admin Access to Bulgarian [events company] Website
Access Type: Website Admin Account
Country: Bulgaria
Revenue: [figure removed]
Price: €50
```

HELD	The offer and the price.
NOT ESTABLISHED	Whether the account works, any sale.

EVIDENCE CARD B13 — 29 Apr 2026

wat4ri Hacker-forum Telegram chat · Telegram · English

ORIGINAL

```
i have acess to a [Bulgarian bank] dev portal is it even
worth selling? lol
```

HELD	The chat message.
NOT ESTABLISHED	Any access; which portal; any sale.

4.7 What the forums add

Forums contributed only 165 tagged posts, but they carry the most specific claims: insurance, retail and health-platform databases, the government mail panel and the combolist series. Many other forum hits are global lists that include Bulgaria among dozens of countries. Buyers also posted requests: "looking for a leak for Slovakia and Bulgaria" (June and September), Bulgarian ID-document sets for verification fraud (September and November) and Bulgarian bank accounts (Chapter 8).

KEY TAKEAWAYS

01

Raw volume is mostly multi-country advertising; read the Bulgaria-specific set.

02

Insurance customer data with national personal numbers was the year's most significant data claim, and the regulator confirmed breach notifications from three insurance companies in two groups.

03

Government-themed posts are about mailboxes and access; treat a cheap "panel" as an unverified access offer and, as a planning choice, review mail-administrator sign-ins.

CHAPTER 5

Targeting examples by sector

THIS CHAPTER ANSWERS

Which Bulgarian sectors are named in criminal, political and official reporting in 2026, and what kind of response does each one need?

9

sectors with observed activity, from government to agriculture

IN SHORT

The posts and reports below show how criminals, hacktivists and authorities described activity against Bulgarian organisations in 2026. Most dark-web examples are claims; rows also cite official reports, marked with their section. Insurance, government and telecom carried the most specific claims; banking carried the most fraud tooling. Verify each claim with the organisation concerned before escalating, and start with the sector's first response.

Victims are described by role under the policy in Appendix A.9.

Government (espionage and mail)

`Espionage` `threat e-mail`

EXAMPLE OF OBSERVED ACTIVITY (ANONYMISED)

A years-long intrusion into state document-exchange networks, officially disclosed (§7.2); local officials' mailboxes accessed, per researchers cited by Reuters (§7.2); bomb-threat e-mails from hijacked accounts (§4.5)

WHAT IT MEANS

Mail and document exchange are the exposed layer; the official account reported no exposure of citizens' personal data

FIRST RESPONSE

Central logging and look-back hunts in mail and document systems; review mail-administrator sign-ins

Government (claims and outages)

`Access claims` `outage report`

EXAMPLE OF OBSERVED ACTIVITY (ANONYMISED)

A "government data" forum claim days after the first disclosure (Case B); a government mail panel for 10 USD (Case C); two state websites reported unreachable on election day (§6.3); network addresses of a state transport-sector system posted (§4.5)

WHAT IT MEANS

The claims are unverified; the cause of the outage remains open

FIRST RESPONSE

Verify claims before comment; pre-agree service-status statements (§6.6)

Insurance

`Data claims` `breach notifications` `extortion listings`

EXAMPLE OF OBSERVED ACTIVITY (ANONYMISED)

At least three offers of insurance customer data (Aug-Sep) and breach notifications from three insurance companies in two groups confirmed by the regulator (Case A); an insurer and its parent holding on a ransomware leak site (Jul, §7.4)

WHAT IT MEANS

Advertised customer identity data with national personal numbers; authenticity unverified

FIRST RESPONSE

Compare samples with export schemas; review portal and partner API access

Banking and payments

`Mule accounts` `carding` `access claim` `phishing`

EXAMPLE OF OBSERVED ACTIVITY (ANONYMISED)

Accounts with Bulgarian IBANs bought and sold for 40-250 USD; a buyer listing nine Bulgarian banks (§8.1); card-checker output naming 15 issuers (§8.2); a claimed bank developer-portal access (Case F); Smishing Triad arrests (§7.7)

WHAT IT MEANS

Fraud tooling dominates; the intrusion-relevant exposure is in device and listing data (Chapter 9)

FIRST RESPONSE

Triage current listings, then employee devices; alert on BIN checker declines

Telecom and internet services

`Credential lists` `extortion listing` `company-disclosed incident`

EXAMPLE OF OBSERVED ACTIVITY (ANONYMISED)

Recurring webmail "valid" and "cracked and inboxed" lists, and mail-checker tools that name a leading Bulgarian webmail service (Case D); a ransomware listing against an internet services company (§7.4); unauthorised access to a large hosting provider's customer system, disclosed by the company (Nov, §7.6)

WHAT IT MEANS

Personal webmail credentials are traded monthly and reused into work systems

FIRST RESPONSE

Block personal webmail for corporate sign-up; require MFA

Retail and e-commerce

`Data claims` `extortion listings`

EXAMPLE OF OBSERVED ACTIVITY (ANONYMISED)

An online retailer database of "around 4M records" (Feb); a furniture retailer's customer data reported for sale (Feb); a trading company and a pharmacy chain on leak sites (§7.4)

WHAT IT MEANS

Customer contact data feeds order-themed phishing

FIRST RESPONSE

Check bulk exports and API logs; warn customers

Health

`Data claim` `extortion listing`

EXAMPLE OF OBSERVED ACTIVITY (ANONYMISED)

A health-care platform database offered two days after its claimed breach date (Jan, Case E); a pharmacy chain on a leak site (Sep)

WHAT IT MEANS

Health-platform data adds birth dates and contact details to identity fraud

FIRST RESPONSE

Review platform export logs and admin access

Media

`Web intrusion (charged)` `DDoS claim`

EXAMPLE OF OBSERVED ACTIVITY (ANONYMISED)

The websites of the public broadcasters BNT and BNR, named by prosecutors among sites a suspect accessed (Oct, §7.7); a sports news portal in a DDoS claim (Mar, §6.2)

WHAT IT MEANS

Media sites hold subscriber and contact databases and are symbolic targets

FIRST RESPONSE

Patch the content-management system (CMS); monitor database exports

Transport and logistics

`Extortion listing` `impersonation` `reconnaissance claim`

EXAMPLE OF OBSERVED ACTIVITY (ANONYMISED)

A logistics firm on a leak site (Jul, §7.4); SMS phishing in the name of couriers (§8.5); network addresses of a state transport-sector system posted (§4.5)

WHAT IT MEANS

Couriers recur in reported SMS-phishing campaigns

FIRST RESPONSE

Publish official sender IDs; request look-alike take-downs

Agriculture and facilities

`OT and device access claims`

EXAMPLE OF OBSERVED ACTIVITY (ANONYMISED)

A greenhouse operator panel claimed by Z-Pentest, which a joint advisory lists among pro-Russia hacktivists (Oct, §6.4); 140 camera logins offered (Aug, Case F)

WHAT IT MEANS

Poorly secured internet-facing panels and cameras are targets for opportunistic access claims

FIRST RESPONSE

Remove default credentials; take management interfaces off the internet

Reading across sectors. Organisation-specific claims fall into three groups. Data sellers name insurers, retailers and health platforms and claim customer databases. Ransomware groups name mid-sized companies across sectors. Political actors claimed little against Bulgaria in our data, and the most consequential state-level activity was reported by the government itself, not claimed by anyone.

KEY TAKEAWAYS

01

Insurance carried the year's most significant data claims, and the regulator confirmed breach notifications from three insurance companies in two groups.

02

Government exposure sits in mail and document exchange, not in claimed population databases.

03

For banks and telecoms, fraud tooling and credential lists dominate the posts; intrusion-relevant exposure sits in device and listing data (Chapter 9).

CHAPTER 6

Hacktivism, DDoS and disruption claims

THIS CHAPTER ANSWERS

Who claimed disruption against Bulgaria in 2026, what did the authorities say, and how should an organisation prepare for the next claim?

2

hacktivist claim sets in our data, both relayed by third parties

INSIDE THIS CHAPTER

6.1 Timeline | 6.2 The March DDoS claims | 6.3 Election day, 19 April | 6.4 An operational-technology claim | 6.5 What we did not see | 6.6 Lessons for defenders

IN SHORT

Hacktivist claims against Bulgaria were sparse in our 2026 data. We saw two DDoS claims with a message about Gaza in March and a Z-Pentest claim of control over a greenhouse panel in October, all through relays. On the April election day the ministry first reported no denial-of-service attacks; press later reported two state websites unreachable for hours. Pre-agree who confirms service status, and take control panels off the internet.

6.1 Timeline

5 Mar 2026 — **TheGarudaEye**
Claims a ministry website "down", with an availability-check link and a message about Gaza; relayed by an onion-links channel

6 Mar 2026 — **TheGarudaEye**
Claims a sports news portal "down" with the same message

16 Apr 2026 — **Ministry of Interior**
Reports that its cybercrime unit took part (13 April) in a Europol-coordinated operation against DDoS-for-hire services: 75,000+ users identified, 4 arrests, 53 domains closed

19 Apr 2026 — **E-government ministry**
Election day: no heightened cyber activity against strategic sites and no denial-of-service attacks reported in the afternoon

19 Apr 2026 — **Press (News.bg, citing Nova)**
Ministry and Council of Ministers websites reported unreachable after a cyberattack; restored shortly after 19:00

7 Jul 2026 — **Press (BNR)**
Bomb-threat e-mails over two days. The first wave reached courts, prosecutors' offices and municipalities in more than 22 cities; hospitals and tax offices followed on the second day. Investigators call it an "automated hybrid attack"

9 Jul 2026 — **CERT Bulgaria**
Bomb-threat e-mails sent to state institutions from hijacked accounts since 6 July

17 Sep 2026 — **State Agency for National Security**
Additional cybersecurity instructions for all strategic sites before the 25 October election

14 Oct 2026 — **Z-Pentest / Z-Alliance**
Claims control of a greenhouse automation panel in Bulgaria and says it renamed the device; relayed by a Spanish-language channel

Dark markers are actor posts, outlined markers are relays by third parties, coral markers are official statements. Dates are post or statement dates; Sofia time is UTC+2 (UTC+3 in summer).

6.2 The March DDoS claims

On 5 March a channel that republishes links to onion sites relayed a post headed "GLOBAL CYBER ATTACK #0070". It claimed a Bulgarian ministry's website was "DOWN by TheGarudaEye" at 08:36 local time, with an availability-check link as proof. The message criticised international plans for Gaza. On 8 March the same channel relayed a second claim, against a sports news portal, dated 6 March [S1].

EVIDENCE CARD B10 — 5 Mar 2026

TheGarudaEye (relayed) Onion-links Telegram channel relaying a claim

Telegram · English

ORIGINAL

```
GLOBAL CYBER ATTACK #0070
Target: [a Bulgarian ministry]
DOWN by TheGarudaEye
Server Down: 05/03/2026 (08:36 Bulgaria Time)
Proof: [availability-check link removed]
Message: Building a new Gaza without involving the people of
Gaza and Palestine? [...]
```

Note. The rest of the message is the actor's political rhetoric and is omitted.

HELD	The claim, its time and its framing.
NOT ESTABLISHED	An outage, its cause or duration; that the actor sent any traffic.

What we can establish. That the claims were posted and relayed. An availability-check link can at most record a moment of unreachability from some test locations; it does not show an outage, its cause or its duration. We found no official statement about either site. The framing concerns events outside Bulgaria; Bulgaria appears as one target in a numbered series.

6.3 Election day, 19 April

In a statement reported at 16:12, the ministry then responsible for e-government said there was no increased cyber activity against strategic sites and no denial-of-service attacks. A temporary cybersecurity situation centre was running from 08:00 to midnight [S18]. Later that afternoon News.bg, citing the television channel Nova, reported that the ministry's and the Council of Ministers' websites had lost connectivity after a cyberattack. The ministry said that despite the interruption its systems were working normally. The sites were restored shortly after 19:00 [S19].

Point	Press report	Official account	What remains open
Effect	Two state websites without connectivity for hours [S19]	Systems "functioning normally" despite the interruption [S19]; no denial-of-service attacks reported earlier that day [S18]	Whether the outage was caused by an attack or a connectivity fault
Scope	Ministry and Council of Ministers sites; the interior ministry's site hard to reach in the outlet's own check [S19]	No list of affected sites	Any other sites
Attribution	None	None	Actor and method
Later assessment	Not stated	Only limited cyberattacks observed in the final hours of election day, a caretaker deputy minister said in May [S20]	No technical report published

What it means. On a day of maximum public attention, two state websites were reported unreachable for several hours, and the official account and the press account used different words for it. No actor claimed it in our data. The defensive lesson is the same as for any DDoS claim: a single, pre-agreed public line, given early.

6.4 An operational-technology claim

On 14 October a Spanish-language relay channel reposted a claim by "Z-Alliance" and Z-Pentest, a group the December 2025 joint advisory lists among pro-Russia hacktivists [S68]. It said a Delta-brand operator panel running a greenhouse automation system in Bulgaria was "under our control", and that the device name had been changed to Z-PENTEST [S1].



What we can establish. The claim, the device type it names and the relay. We did not verify it, and neither the owner nor an authority confirmed it as far as we found. Claims of this kind usually concern internet-exposed operator panels with default or no passwords. They are low-cost for the claimant and potentially costly for the owner. In November CERT Bulgaria warned of attacks across Europe on internet-exposed refrigeration controllers [S37], which points to the same weakness.

A threat-intelligence vendor separately reported a 2026 claim by AlfaNet or the Z-Pentest Alliance. The claim was full control of a Rapid SCADA (supervisory control and data acquisition) server tied to energy and gas infrastructure in Bulgaria; the vendor presented it as the group's allegation [S69].

6.5 What we did not see

We found no 2026 claim against Bulgarian targets by the DDoS groups most active in Europe in recent years, beyond those above. Stress-test logs that list Bulgarian hosting ranges appear in our data, but they record test traffic, not claimed campaigns.

Absence from our collection does not mean absence of attacks: claims in closed channels, and attacks that no one claims, are invisible here. A repeat search of public reporting in English, Bulgarian, Russian and Turkish found no reputable report of a hacktivist DDoS campaign against Bulgarian targets in 2026. On 19 November the minister said attacks on government websites were continuing and were being blocked, without naming a claimant [S61].

6.6 Lessons for defenders

1. **Pre-agree the public line.** On election day the press and the ministry described the same interruption differently. Decide in advance who confirms service status, within what time and through which channel.
2. **Protect portals upstream.** Citizen-facing portals need contracted DDoS mitigation before an election or a high-profile date, not during it.
3. **Take operator panels off the internet.** Greenhouse, refrigeration, building and camera controllers should sit behind a VPN with non-default credentials.
4. **Expect threat e-mail from real mailboxes.** The July bomb-threat e-mails came from hijacked accounts that passed mail authentication [S35]. The first wave reached courts, prosecutors' offices and municipalities in more than 22 cities, and hospitals and tax offices followed [S72]; train

staff and have a reporting route.

KEY TAKEAWAYS

01

Hacktivist claims against Bulgaria were few in our 2026 data and none was confirmed by the affected organisation or an authority.

02

On election day two state websites were reported unreachable for hours while the ministry said its systems worked normally; a pre-agreed public line closes that gap.

03

Poorly secured internet-facing panels are targets for opportunistic access claims.

CHAPTER 7

Threat actors

07

THIS CHAPTER ANSWERS

Who is behind the activity, how are the actors connected, and what does the official record say about each of them?

19

ransomware leak-site listings for Bulgaria in 2026 after review, naming 17 organisations

INSIDE THIS CHAPTER

7.1 How the actors connect | 7.2 Espionage against state networks | 7.3 Hacktivist and disruption claimants | 7.4 Ransomware and extortion
7.5 Criminal personas seen in Blackhole | 7.6 An incident disclosed by a company | 7.7 Officially reported operations and arrests

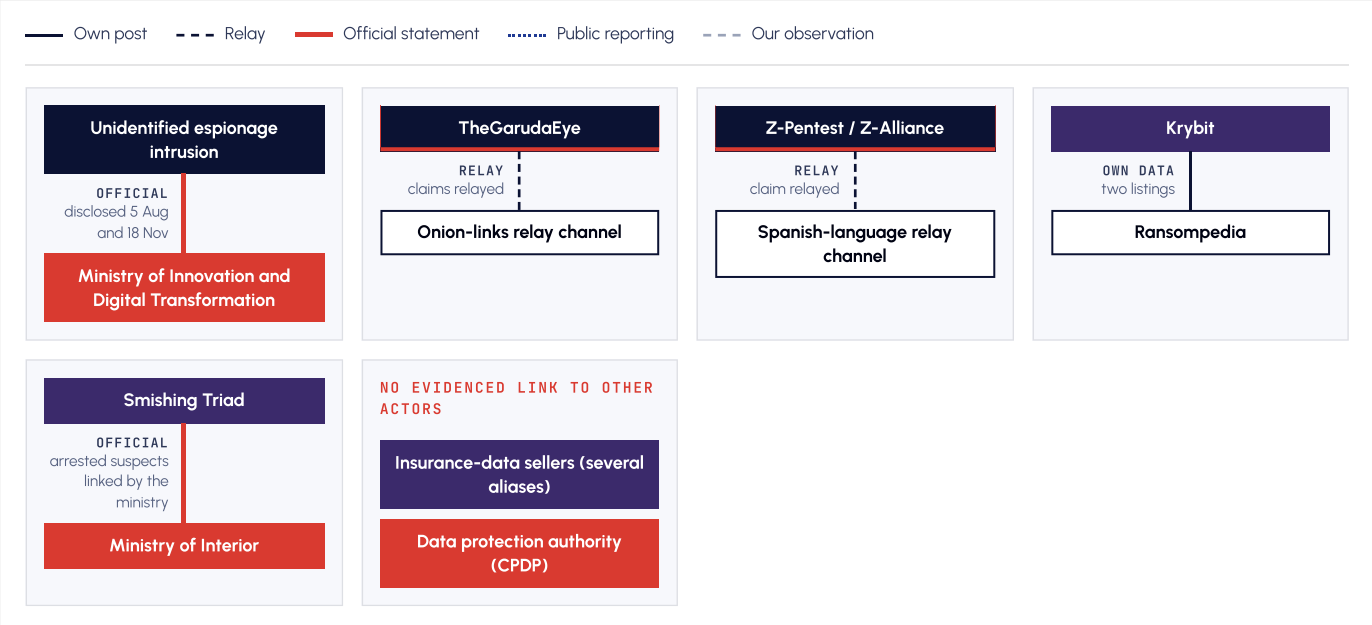
IN SHORT

Five actor types matter for Bulgaria in 2026. An unidentified intrusion set spent years inside state document-exchange networks, by the government's account. Ransomware groups posted 19 listings naming 17 Bulgarian organisations, against 7 listings in 2025; coverage changes, so this is not a growth rate. Criminal sellers trade Bulgarian identity, account and credential data. Hacktivists claimed little. Police cases add phishing and fraud networks, some international. Hunt for long-lived access in mail and document systems first, then rehearse extortion.

Each profile separates **observed behaviour**, **the actor's own claim**, **what remains unresolved** and **what it means for organisations**. Confidence applies to a specific proposition, not to the actor as a whole.

7.1 How the actors connect

The map links actors only where we hold evidence, and each line says what kind: a third-party relay, an official statement or our own data. A line is an association, not proof of a common operator.



The "Starred Bears" forum claim (Case B) appeared days after the first disclosure; nothing links it to the intrusion, so the map draws no line between them. Three insurance companies in two groups notified the data protection authority of breaches (§4.4); no offer has been matched to any notification, so the map draws no line there either.

7.2 Espionage against state networks

Unidentified espionage intrusion

No public name

Cyber-espionage (officially reported)

Not attributed; the minister said several international hacking groups were believed involved and that no conclusive link to a state was found

IN BULGARIA, 2026

5 Aug	Ministry discloses unauthorised access to administrative networks, possibly lasting years
18 Nov	Ministry says access since 2021 to state document-exchange infrastructure was cut off in three phases
18 Nov	Minister gives at least 130 GB, more than 62 million pages; minister says prosecutors were asked to examine state bodies' actions in that period

CLAIMED TARGETS

Infrastructure through which state institutions exchange documents and information

SEEN IN PUBLIC REPORTING

- [S22] Ministry of Innovation and Digital Transformation: unauthorised access found during deployment of the national cybersecurity system
- [S23] Ministry: access since 2021; no exposure of citizens' personal data found so far; 90-day enhanced monitoring
- [S24] Mediapool: minister says groups' motives and links unknown; no information that documents appeared on the dark web
- [S25] Reuters: no conclusive evidence linking the attackers to a particular state

OUR ASSESSMENT

The most consequential intrusion of the year by the government's account. Entry route, tools and actors are not public, and nothing in our dark-web data can be tied to it.

CONFIDENCE **High that the government reports a years-long intrusion; actor and method unresolved**

The government's account is the only public source on this intrusion, and it has been given in stages. On 5 August the ministry said it had found unauthorised access to certain administrative networks while deploying the new national cybersecurity system [S22]. On 18 November it said the access had lasted since 2021 and touched the infrastructure through which institutions exchange information. It said the attackers had been cut off and removed in three phases, and that the affected infrastructure would stay under enhanced monitoring for 90 days [S23].

At a briefing the same day the minister gave the volume as at least 130 GB, more than 62 million pages, covering most areas of state administration. He said several international hacking groups were believed to be involved. He said it was not established whether they acted alone, together or for foreign intelligence services, and that he had no information that the documents had appeared on the dark web [S24][S25]. The minister said the prosecutor's office had been asked to examine the actions of state bodies during that period [S25].

Unresolved. The entry route, the tools, the actors and whether any data has been used. **Meaning.** By the government's account, a document-exchange layer was readable for about five years; the minister said the new national system gave a unified picture for the first time [S24]. For any organisation that exchanges documents with the state, the decisive controls are central logging, administrator-account control and hunting for long-lived access, not perimeter alerts. Nothing in our 2026 dark-web data can be tied to this intrusion (Case B, §4.6).

Other 2026 espionage reporting that names Bulgaria. Two further reports concern Bulgarian targets, each with its attribution stated by the source.

Date	Reported by	What the source says	Attribution as stated
15 Apr	Reuters, relayed by Fakti	On an exposed attacker server, researchers found evidence that at least four mailboxes of local officials in the Plovdiv region had been accessed, within a campaign that reached at least 284 mailboxes between September 2024 and March 2026; Bulgarian authorities did not respond [S67]	The researchers attribute it to Fancy Bear (APT28); ESET could not confirm that, and a second vendor disputed it [S67]

Date	Reported by	What the source says	Attribution as stated
4 Nov	Sekoia; reported by Ruse.news on 5 Nov	A website in Bulgaria's military sector was one of several sites where attackers tampered with a JavaScript library to send visitors' phones to exploits for already-patched (n-day) flaws; Sekoia did not say whether any visitor was exploited [S66]	APT29, with moderate to high confidence, according to Sekoia [S66]

Meaning. Both cases reach people through tools they trust: a webmail inbox and a familiar website on a phone. Mail-account monitoring, phishing-resistant MFA and prompt mobile updates are the controls these reports point to.

7.3 Hacktivist and disruption claimants

TheGarudaEye

Hacktivist (DDoS claims)

Framing about Gaza in its own messages; no reputable public profile found

IN BULGARIA, 2026

5 Mar	Claims a ministry website down (B10)
6 Mar	Claims a sports news portal down

CLAIMED TARGETS

A ministry website and a sports news portal

IN THEIR WORDS

> *"GLOBAL CYBER ATTACK #0070"* B10

SEEN IN PUBLIC REPORTING

OUR ASSESSMENT

A numbered series of claims in which Bulgaria is one target; proof consists of availability-check links. We found no reputable public reporting on the group.

CONFIDENCE **High that the claims were posted and relayed; effect unverified**

Z-Pentest

Presented as part of "Z-Alliance"

Hacktivist (OT access claims)

Listed among pro-Russia hacktivist groups in joint advisory AA25-343A [S68]

IN BULGARIA, 2026

14 Oct	Claims control of a greenhouse automation panel in Bulgaria (B11)

CLAIMED TARGETS

An internet-exposed operator panel of a commercial greenhouse

IN THEIR WORDS

> *"Acceso concedido, Bulgaria"* B11

SEEN IN PUBLIC REPORTING

- [S68] Joint advisory AA25-343A (Dec 2025): named among pro-Russia hacktivist groups that use poorly secured internet-facing VNC (remote-desktop) connections to reach OT control devices
- [S69] KELA (2026): AlfaNet or the Z-Pentest Alliance claimed control of a Rapid SCADA server tied to energy and gas infrastructure in Bulgaria; presented as the group's allegation

OUR ASSESSMENT

A relayed claim about an operator panel, consistent with the group's reported focus on internet-exposed OT. Its Bulgarian claims were not confirmed by the affected organisation or an authority.

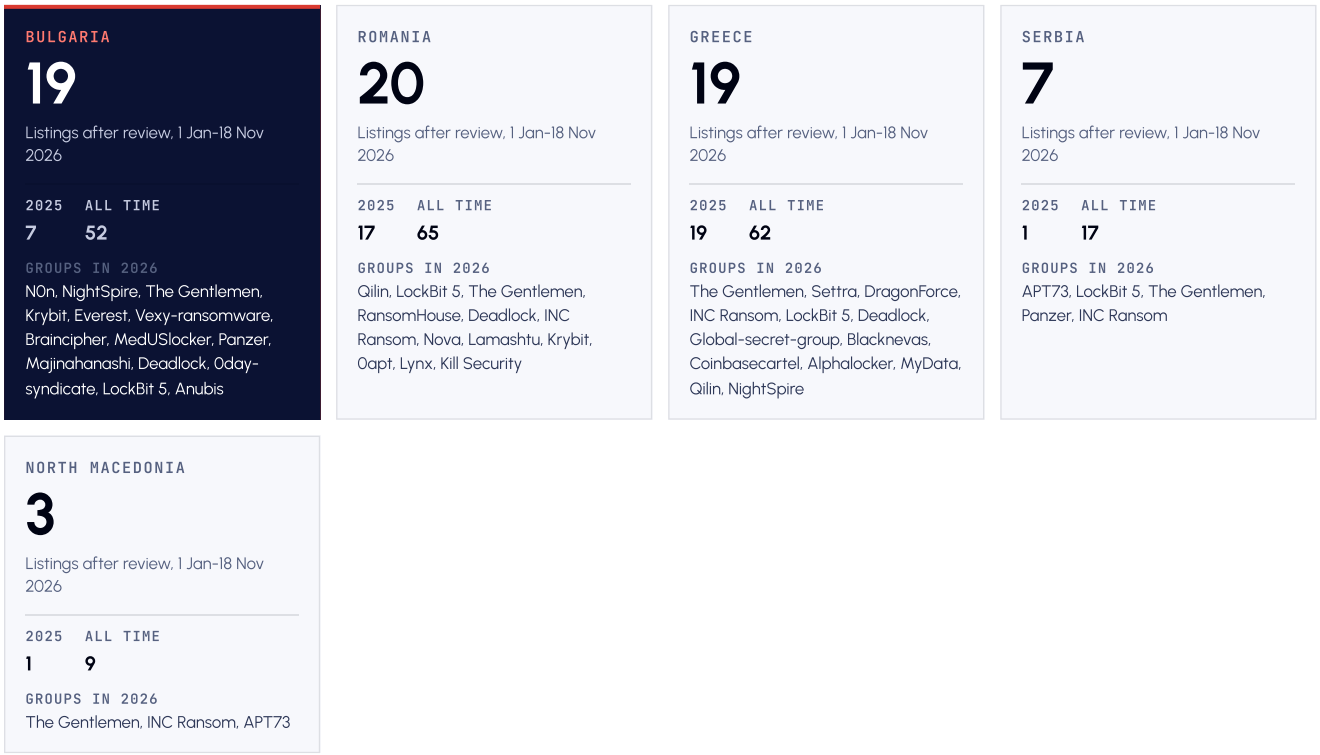
CONFIDENCE **High that the claim was relayed; access unverified**

Neither claimant's activity against Bulgaria was confirmed by the affected organisation or an authority. Joint advisory AA25-343A, issued in December 2025 by CISA, the FBI and international partner agencies, names Z-Pentest among pro-Russia hacktivist groups that use poorly secured,

internet-facing remote-access (VNC) connections to reach operational technology [S68]. We found no reputable public profile of TheGarudaEye. The election-day outage of two state websites (§6.3) was not claimed by any actor in our data.

7.4 Ransomware and extortion

Ransompedia holds 19 Bulgarian listings in 2026, close to Romania and Greece and well above Serbia and North Macedonia



Source: Brandefense Ransompedia listings after review, all dates, to 18 November 2026 [S6]; ransomware.live as a cross-check [S7].

After review, Ransompedia holds 19 listings naming Bulgarian organisations between 1 January and 18 November 2026, against 7 in the whole of 2025 and 52 in total. Two organisations were listed twice, so the 19 listings name 17 organisations. Romania has 20 listings in the same window, Greece 19, Serbia 7 and North Macedonia 3 [S6]. The listings fall in January (3), May (2), July (5), September (5) and October (4).

Item	2026 value
Groups	14, led by Krybit, N0n, NightSpire, The Gentlemen and Everest with two listings each
Sectors (Ransompedia labels)	Education 3, finance 2, health 2, entertainment 2, technology 2; one each in retail, media, IT services, logistics, food and drink and hospitality; two in other or cross-sector labels
Listed organisations by role (examples)	A holding company and its insurance subsidiary (July, one group, one day apart); a trading company; a gaming-technology maker; a pharmacy chain; an office-equipment provider; an internet services company
Claims not counted	Three relayed or tracker claims were not counted after review, including one that a public tracker [S7] labels Bulgarian and Ransompedia records as Serbian

Krybit

`Ransomware and data extortion` `Financially motivated`

IN BULGARIA, 2026

Jul	Lists an insurance company on its leak site
Jul	Lists the insurer's parent holding (B18)

CLAIMED TARGETS

A holding company and its insurance subsidiary

IN THEIR WORDS

> *"krybit claims attack"* B18

SEEN IN PUBLIC REPORTING

- [S6] Ransompedia: two Bulgarian listings in 2026, both in July; one Romanian listing in the same window
- [S70] Cyble: financially motivated ransomware-as-a-service built on leaked Babuk code, first seen in March 2026; Bulgaria not mentioned

OUR ASSESSMENT

The only group with two Bulgarian listings from the same corporate group. The listings are claims; neither company had confirmed an incident by our cut-off as far as we found.

CONFIDENCE **High that the listings exist; any intrusion unverified**

EVIDENCE CARD B18 — 19 Jul 2026

Leak-monitor bot Leak-monitor Telegram bot relaying a ransomware tracker

Telegram · English

ORIGINAL

```
"Victim": "[holding company]",
"Content": "Ransomware group called krybit claims attack for
[holding company]. [...]"
"Type": "Ransom Alert"
```

Note. The same group also listed the holding's insurance subsidiary (§7.4).

HELD	That the group listed the holding on its leak site, as relayed.
NOT ESTABLISHED	Any intrusion, encryption or data theft; any negotiation.

Cyble describes Krybit as a financially motivated ransomware-as-a-service operation built on leaked Babuk code, first seen in March 2026; its profile does not mention Bulgaria [S70].

What this means. A listing is a criminal's claim that it holds data and that a victim did not pay. It is not proof of a breach or of encryption, and none of the 17 organisations had confirmed an incident by our cut-off as far as we found. The 2026 count is high against the previous year, but Ransompedia coverage and group behaviour change, so we do not read it as a growth rate.

It does show that ransomware groups publish Bulgarian organisations in numbers comparable with Romania and Greece. In July the Interior Minister also named ransomware against company networks among the threats the police see [S38]. For 2025, the EU cybersecurity agency counted Bulgaria among the least targeted member states, with 0.3% of EU ransomware claims [S64]; the 2026 listings sit against that low base.

7.5 Criminal personas seen in Blackhole

Aliases only; no contacts, links or real identities.

Persona or brand	Observed role in 2026	Own claim	Unresolved
thejackal101	Combolist poster on several forums; "Database: Bulgaria" lists (Jan-Oct)	68,000-126,000 "fresh" lines per list	Origin, overlap, validity (Case D)
Max_Leaks / Maxleak	Combolist brand on two forums (Apr-Sep)	56,000-150,000 lines per list	Same as above
kookiegst	Poster of webmail "hits" lists (Aug)	"Freshly cracked and inboxed" accounts	Validity

Persona or brand	Observed role in 2026	Own claim	Unresolved
DuperKinger123	Forum seller of government mail panels for several countries (Apr)	Bulgarian government mail panel, 10 USD	Any verification (Case C)
lauraallen	Forum seller of a "Bulgaria insurance database" (Sep)	Sample header with national personal numbers	Origin (Case A)
Intelligence	New forum account that offered data attributed to an insurer, per press (Sep)	3.1 million rows	Any verification [S32]
Enigma Group	Poster of network addresses of a state transport-sector system (Aug)	Backend VPN and WAN addresses	Any access
Commando	Seller of an events company's website admin account (Feb)	Admin access, 50 EUR	Any verification
X FORUMS (bot)	Automated uploader of small credential files, including Bulgarian domains	None	Not a person; a distribution bot

7.6 An incident disclosed by a company

On 17 November a large Bulgarian hosting provider said it had detected unauthorised access to one of its internal systems, as reported by Money.bg. Customer profile data was involved: names, e-mail addresses, phone numbers and billing details including personal or company identification numbers. The company said hosting services were not affected, passwords were stored hashed and some were reset as a precaution, and it had no indication so far of customer data leaking. It said it had notified the data protection authority and CERT Bulgaria [S65]. Its manager said the attack was probably made by an automated AI agent; that is the company's own assessment [S65].

Meaning. A hosting provider's customer database names the people who administer thousands of Bulgarian websites. Its customers should expect phishing that quotes their real account details, and should enable MFA on their hosting accounts.

7.7 Officially reported operations and arrests

The posts show offers; the official record shows people being arrested. Five 2026 cases stand out because they name the method.

Date	Reported by	What happened
14 Mar	Ministry of Interior	Cybercrime officers arrested two foreign nationals buying smartphones in Sofia with other people's payment cards; the ministry said their involvement in the international "Smishing Triad" group had been established [S39]
16 Apr	Ministry of Interior	The cybercrime unit took part (13 April) in a Europol-coordinated operation against DDoS-for-hire services in 20 countries: more than 75,000 users identified, 4 arrests, 53 domains closed [S56]
6-21 Apr (detentions 9 May)	Ministry of Interior	Senders of tens of thousands of phishing messages in the name of the ministry, other institutions and courier companies were identified; they used AI and an Asian platform to generate and send them; two people were detained [S41]
28-30 Oct	Prosecutor's Office	A 19-year-old was charged with unauthorised access to the websites of state and municipal institutions, companies and two national public broadcasters, copying databases of names, phone numbers, personal ID numbers and addresses, and offering data for sale on hacker forums [S42]
13 Nov	Ministry of Interior	The cybercrime unit took part in Operation Endgame against Gootloader, CastleRAT and StealC: 235 servers and 257 domains seized and more than 6 million victim data sets identified [S43]

Smishing Triad — `SMS-phishing network`

`Financially motivated; described by the Interior Ministry as an international organised crime group`

IN BULGARIA, 2026

14 Mar — Two suspects arrested in Sofia buying smartphones with other people's cards; ministry says their involvement in the group was established

CLAIMED TARGETS

Bank-card holders, through phishing messages that lead victims to hand over card details

SEEN IN PUBLIC REPORTING

- [S39] Ministry of Interior: the group operates in more than 120 countries according to public data; its phishing messages lead victims to give their bank details

OUR ASSESSMENT

The only international phishing network that Bulgarian police linked by name to a 2026 arrest. The case connects SMS phishing to in-store purchases with stolen card details.

CONFIDENCE **Medium: link stated by the ministry; no court finding yet**

What this tells defenders. Two of the five cases are international operations in which Bulgarian police took part; the other three were run against people operating in or from Bulgaria. The October case shows that a single actor can reach state, municipal, media and company websites. Prosecutors named the two public broadcasters, BNT and BNR, among the sites. That makes web-application patching and database-export monitoring a government and media control, not only an e-commerce one.

KEY TAKEAWAYS

01

By the government's account, the most consequential intrusion of the year was espionage in state document-exchange networks, detected after about five years.

02

Ransomware groups posted 19 Bulgarian listings, in numbers comparable with Romania (20) and Greece (19); listings are claims, not confirmed breaches.

03

Police cases name methods that defenders can test: AI-written phishing, phones bought with other people's cards, and web intrusions that end in data sales.

CHAPTER 8

The fraud economy

THIS CHAPTER ANSWERS

How do criminals turn Bulgarian identities and accounts into money, and what do the police cases show about the methods that work?

110 USD

median asking price for a bank or payment account in reviewed posts

INSIDE THIS CHAPTER

8.1 Bank and payment-account trading
8.2 Card material in posts: a narrow view
8.3 Identity, KYC and SIM services
8.4 Prices in context
8.5 What police and supervisors reported

IN SHORT

Identity documents and bank and payment-account trading are the largest Bulgaria-specific crime categories in our data, followed by card-checker output. Bulgarian IBANs, fintech accounts and ID-card sets are offered at asking prices of tens to a few hundred dollars. The police cases of 2026 describe SMS phishing in the name of the police and couriers, call-centre investment fraud and, in one case, a loan taken after a bank-profile contact-detail change. Confirm payment instructions out of band, and assume identity data is known.

8.1 Bank and payment-account trading

Account trading is the second-largest Bulgaria-specific crime family in our data, after identity documents (291 distinct posts against 341; 2,040-2,151 in the reviewed tagged set). Buyers and sellers trade accounts with Bulgarian IBANs at banks and payment institutions, often as "ready" or "verified" accounts. Observed asking prices include 40 USD for a verified payment-service account (January), 100 USD for a ready account at a Bulgarian bank (March) and 200-250 USD for the same bank's accounts (August-September). One seller offered "5-10 accounts per day" at another bank (February), and a July buyer listed nine Bulgarian banks it wanted accounts from.

The risk these offers create for banks is not a hack of the bank but mule accounts: accounts opened or rented under real identities that later carry fraud proceeds. The posts show the offers, not that any account was opened or used at a named bank.

EVIDENCE CARD B14 — 12 Jul 2026

mansorryuwu Telegram registrations and jobs chat · Telegram · English

ORIGINAL

```
WTB BULGIRA
1 [bank]
2 [bank]
3 [bank]
4 [bank]
5 [bank]
6 [bank]
[...]
```

Note. "WTB" means "want to buy". The buyer listed nine Bulgarian banks; names are removed.

HELD	Demand for accounts at Bulgarian banks.
NOT ESTABLISHED	Any account opened, sold or used.

8.2 Card material in posts: a narrow view

> **SCOPE OF THE CARD FIGURES**
>
> The card figures in this report cover only payment cards that appeared in clear text inside the dark-web posts we collected for this report. Brandefense detects stolen cards through many other methods, which this report does not cover. These figures are not a measure of card theft or fraud loss in Bulgaria.

Within that narrow scope, 126 distinct Bulgaria-associated cards appeared in clear text in collected posts. Of these, 81 were attributed to one of 15 named Bulgarian banks and payment institutions, and 45 were labelled only as Bulgarian, without an issuer. Card-checker output carried 115 of them, and 114 were seen in January-April [S8]. The useful signal for issuers is the checker pattern: batches of cards tested with small authorisations against merchant gateways (Chapter 9).

8.3 Identity, KYC and SIM services

KYC and document posts (341 Bulgaria-specific; 1,567-1,672 in the reviewed tagged set) offer verified accounts at exchanges and payment services, "Bulgaria ID front and back and selfie available in bulk" (November), and document-rendering services. Buyers asked for Bulgarian document sets "on a permanent basis" (September) and for Bulgarian KYC (May). In April police in Plovdiv seized a computer holding more than 1,000 scanned Bulgarian ID cards during election-related checks [S44]. SMS-sending software covering 32-33 countries, Bulgaria among them, was advertised in October. Combined with the identity data in §4.4, these services lower the cost of opening accounts in someone else's name.

EVIDENCE CARD B15 — 5 Nov 2026

annabelle0 Cracking forum · Forum · English

ORIGINAL

```
Bulgaria ID Front and Back and selfie available in bulk,
Telegram JOIN KYC BYPASS CHAT [links removed]
```

HELD	The offer.
NOT ESTABLISHED	Whether the documents are genuine, stolen or fabricated; volume.

8.4 Prices in context

Product (reviewed posts)	Median asking price	Spread
Bank or payment account	110 USD	55-230 USD
KYC or document service	100 USD	50-200 USD
Combolist	50 USD	20-400 USD
Access offer	400 USD	Wide, few values
Government mail "panel" (single offer)	10 USD	Single offer
Website admin account (single offer)	50 EUR	Single offer

Prices are asking prices from the minority of posts that quote one; they do not measure market value or completed sales. Spread is the middle half of quoted prices (25th to 75th percentile), not the full range.

8.5 What police and supervisors reported

The posts show offers. The reports below describe attempted and reported frauds; all were published in 2026, and none appeared in our Blackhole data.

Date	Reported by	What happened
7 Jan	Financial Supervision Commission	E-mails in the commission's name told recipients that a foreign transfer needed an extra fee to complete [S45]
23 Jan	Ministry of Interior	A January rise in scams against sellers on classified-ad sites: a fake buyer sends a phishing link asking for card data and 3-D Secure codes; dozens of complaints [S40]
3 Feb	Financial Supervision Commission	Managers of crypto-asset firms were entered in the commercial register with forged documents, without the owners' knowledge, enabling loans in the firms' names [S46]
8 May	Ministry of Interior	Mass SMS and app messages in the ministry's name about unpaid speeding fines "with a 30% discount", linking to look-alike domains [S47]
18 May; 11 Nov	CERT Bulgaria	SMS phishing impersonating the Interior Ministry, the traffic police and the transport ministry over fines and parking fees, with nearly 30 malicious domains listed in May; further SMS from international numbers in November [S48][S49]
3 Jun	Ministry of Interior, as reported by BNR	The head of the cybercrime unit's cyber-intelligence department said three to four Bulgarian companies a week fall victim to fraud in which payee IBANs are replaced or business e-mail is accessed, with single losses of 1-5 million EUR [S62]
10 Jun (published; operation date unclear in the release); 21 Oct	Ministry of Interior	Call centres running investment fraud against foreigners were shut down in Sofia, and four call centres in Varna, Burgas and Sofia using AI-generated crypto platforms; damage of 600,000 EUR in the October case [S50][S51]
19 Jun	Prosecutor's Office	A suspect used the victim's own mobile phone to change the bank-profile contact phone and e-mail, then applied for a 25,000 EUR loan in the victim's name through the bank's electronic channel; the bank bore the loss [S52]
14 Aug	Communications Regulation Commission and the three mobile operators	Joint action against a rise in caller-ID spoofing scams; the regulator said spoofing cannot be stopped by blocking numbers alone [S63]
28 Aug	Ministry of Interior	Fake "police summons" e-mails used police and Europol logos and the names of police leaders to accuse recipients of crimes [S53]
19 Nov	Ministry of Interior	The cybercrime unit said it receives more than 100 reports a day of hijacked accounts and apps [S54]

What this tells defenders. The police cases that state amounts describe payee-IBAN fraud against companies, investment call centres and, in one case, a loan taken after a contact-detail change, not the database sales that dominate dark-web headlines. The SMS waves impersonate the institutions citizens are most likely to obey: the police, the transport ministry and couriers. The controls are procedural and technical: out-of-band confirmation of contact-detail and payee changes, step-up checks for loans after any profile change, take-down of look-alike domains, and customer warnings timed to each wave.

KEY TAKEAWAYS

01

Identity documents and account trading, not card theft, are the largest Bulgaria-specific fraud signals in our data.

02

Card figures cover only cards seen in clear text in collected posts (§8.2).

03

Police cases point to SMS phishing in the name of the police and couriers, investment call centres and, in one case, a loan taken after a bank-profile contact-detail change.

CHAPTER 9

Banking and finance deep dive

09

THIS CHAPTER ANSWERS

Where does the visible exposure of Bulgarian banks sit: in the bank, at its staff, or at its customers?

4 of 16

card-issuing banks with a current credential listing, the first item to triage

IN SHORT

Most visible exposure sits on the customer side: 18,742 non-employee device associations at the 16 card-issuing banks on our list, card-checker output and trading in Bulgarian bank accounts. The bank- and staff-side signals are current listings at 4 of 16 banks and 67 employee-classified devices. Three banks carry two thirds of the customer-device signal. Triage each current listing first, then validate employee devices, and monitor checker declines on your BIN ranges (a BIN is the issuer's card-number prefix).

This chapter covers the 16 card-issuing banks among the 31 banking-and-finance organisations in Chapter 3. The other 15 are the central bank, a development bank, market infrastructure, payment and e-money institutions, consumer lenders, pension funds and a foreign bank's branch. That is why 18,742 non-employee devices here differs from 34,765 there, 67 employee devices from 126, and 4 of the sector's 12 current listings sit at banks. Aggregates only; individual banks are not named.

4 of 16

card-issuing banks with a current credential listing (4 of the sector's 12; the other 8 sit at organisations that do not issue cards)

16 of 16

card-issuing banks with non-employee device associations (18,742 in total; ownership and current infection unverified)

9 of 16

card-issuing banks with employee-classified devices (67 in total)

12 of 16

card-issuing banks enforcing DMARC (20 of 31 across the sector)

12 of 16

card-issuing banks with cards in clear text in collected posts (70 of the 126 cards name one of them; narrow scope, §8.2)

The three banks with the most non-employee device associations account for 66% of them.

What it means for banks.

1. **Current listings come first.** 4 of 16 banks had one on the day of the check; apply Decision 1 (disposition within 5 working days).
2. **Employee exposure is small but real.** 67 employee-classified devices across 9 banks are the intrusion-relevant subset. After current listings, these deserve priority validation over the much larger non-employee total.
3. **Non-employee device associations are the larger exposure.** 18,742 device associations across all 16 banks are not employee-classified, and most plausibly they are customers' devices. Ownership, current infection and whether any stored session or password still works are unverified and require validation. Fraud teams should use device and session risk signals at login and at payee changes, not only password checks.
4. **Card checking is a detectable precursor.** Checker bots test cards with small authorisations or card-add attempts on merchant gateways. Issuers can detect clusters of declined low-value attempts from foreign gateways on their BIN ranges, identify the cards involved, check their authorisation and fraud signals, and reissue the cards confirmed at risk under issuer policy.
5. **Mule accounts and profile takeover are the downstream risk.** Account-trading posts seek Bulgarian bank accounts (§8.1), and one police case describes a loan taken after a victim's contact details were changed from the victim's own phone (§8.5). Onboarding and profile-change controls should assume that EGN, birth date and address are known to criminals (§4.4).

KEY TAKEAWAYS

01

Current credential listings at 4 of 16 card-issuing banks come first, then the 67 employee-classified devices; the 18,742 non-employee ones also need validation.

02

12 of 16 card-issuing banks enforce DMARC; four do not.

03

Card-checker declines on your BIN ranges and changes to customer contact details are detectable precursors.

CHAPTER 10

Regulatory and national response

THIS CHAPTER ANSWERS

What changed in Bulgaria's cyber rules in 2026, and what must an organisation have in place now that the reduced-fine period has ended?

24 h

to send an early warning of a significant incident under the amended Cybersecurity Act

IN SHORT

2026 reset Bulgaria's cyber rulebook. Amendments to the Cybersecurity Act transpose NIS2, with 24-hour early warnings and fines of up to 10 million EUR or 2% of turnover. A 50% fine reduction applied only to violations up to 1 June 2026. A new ministry leads digital government and cybersecurity, and the EU infringement case is closed. Confirm whether you are an essential or important entity, and test your 24-hour reporting route now.

Measure	What we could verify	Status and caution
Cybersecurity Act amendments (NIS2)	Adopted by the National Assembly on 5 February 2026, promulgated by Decree No. 52 of 11 February and published in State Gazette No. 17 of 13 February 2026 [S28]	The published text gives no separate commencement date; several implementing deadlines run from the law's entry into force; we read the obligations as in force, so confirm the commencement date with counsel
Scope	Essential entities are mainly the Annex I types above the medium-enterprise ceiling, plus some categories regardless of size (e.g. administrative bodies, DNS and trust-service providers); important entities are the other Annex I and II types (Art. 4a) [S28]	Entities are identified by the competent authorities after a Council of Ministers decision (§47-48) [S28]
Incident reporting	Early warning within 24 hours of detecting a significant incident, notification within 72 hours, final report no later than one month after the notification (Art. 23(5)) [S28]	Applies to essential and important entities. Trust-service providers notify within 24 hours; an interim report is due on CSIRT request; if the incident is unresolved at one month, an interim report, then a final report within one month of resolution [S28]
Fines: essential entities	Sanction on the organisation of up to 10,000,000 EUR or 2% of worldwide annual turnover, whichever is higher, and not less than 25,000 EUR (Art. 29(2)) [S28]	Art. 29(2) does not apply to essential entities that are administrative bodies (Art. 29(5)). Violations up to 1 June 2026 had fines reduced by 50% (§51); that period has ended [S28]
Fines: important entities and management	Important entities: sanction on the organisation of up to 7,000,000 EUR or 1.4%, and not less than 12,500 EUR (Art. 29(3)). Personal fines of 500-5,000 EUR for heads of administrative bodies, managers and management-body members who breach Art. 21 security measures (Art. 29(4)) [S28]	The same 50% reduction applied up to 1 June 2026 [S28]
Register	The minister responsible keeps a register of covered entities; changes must be reported within two weeks (Art. 6) [S28]	The act names the Minister of e-Government; that ministry was merged into the Ministry of Innovation and Digital Transformation in May [S26]; we could not confirm which ministry now keeps the register
Implementing acts	Within 6 months of entry into force the Council of Ministers designates the competent authorities and adopts the identification method; an ordinance follows within 8 months and a new national strategy within 9 months (§47) [S28]	We could not confirm by our cut-off that each step was taken
EU infringement	The European Commission closed infringement procedure 2024/0257 against Bulgaria after full transposition was notified on 6 March 2026, the ministry said on 1 October [S29]	Closed

Measure	What we could verify	Status and caution
National Cybersecurity System	On 4 November the ministry reported a Council of Ministers decision designating the administrations to be included in the National Cybersecurity System [S60]	The list of administrations was not published in the announcement
DORA	Amendments in the Markets in Crypto-Assets Act make the BNB competent for the credit institutions it supervises and, via the Payment Services and Payment Systems Act, for payment and e-money institutions; the Financial Supervision Commission covers investment firms, insurers, crypto-asset providers and others [S73]	DORA applies from 17 January 2025; the amendments were published in State Gazette No. 54 of 4 July 2025 [S73]; earlier legal commentary [S58] describes the bill at the submission stage; confirm your authority with counsel
Critical entities (CER)	A draft act on the resilience of critical entities went to public consultation from 27 May to 26 June 2025 [S59]	Adoption not confirmed by our cut-off

The new chapter also makes the Cybersecurity Council the cyber-crisis management authority (Art. 17a) and gives the national CSIRT the role of coordinator for coordinated vulnerability disclosure (Art. 19(4)) [S28].

Does the amended act apply to you? The table reads the act's structure [S28] for four common cases; confirm with counsel.

Organisation	Likely regime	Action now
Bank, payment institution, insurer or investment firm	DORA is the EU sector-specific regime for ICT risk and incident reporting at financial entities; check with counsel how the Bulgarian act treats the overlap	Map DORA major-incident reporting to your competent authority (BNB or Financial Supervision Commission), and confirm with counsel any parallel notice to CERT Bulgaria; test it
Energy, transport, health, water, digital-infrastructure or other Annex I organisation above medium size	Essential entity	Register; name the person who sends the 24-hour early warning; record management approval of security measures
Other Annex I or II organisation of at least medium size, including manufacturers, postal and courier services, food and chemicals	Usually an important entity; some types are covered or essential regardless of size (Art. 4, 4a), so confirm with counsel	Same reporting duty; lower fine ceiling
State or municipal administration	Covered by the act and, where designated, by the National Cybersecurity System [S60]	Confirm inclusion in the national system; align logging with it

What CISOs should do now. Confirm in writing whether you are an essential or important entity, and register with the ministry that keeps the register (confirm which with counsel). Name the person who sends the early warning and give them a 24-hour route that works at weekends. Rehearse the 72-hour notification and the one-month final report with a real past incident, including the interim-report path for an unresolved incident. Keep a dated record of management approval of security measures, because management-body members can now be fined for breaches of the security-measure duties. This section is not legal advice.

KEY TAKEAWAYS

01

The NIS2 amendments were published on 13 February 2026, with 24-hour early warnings and fines of up to 10 million EUR or 2% of turnover.

02

The 50% fine reduction applied only to violations up to 1 June 2026.

03

Register, name your incident reporter and test the 24-hour route now.

CHAPTER 11

Outlook

THIS CHAPTER ANSWERS

What should Bulgarian organisations plan for next, and what evidence would change that plan?

5
key judgements, each with a signal to watch

INSIDE THIS CHAPTER

11.1 Key judgements | 11.2 What would change the assessment | 11.3 Conditional scenarios

IN SHORT

Plan for the same evidence types, not a new threat. They are identity exposure that stays invisible until it is used, ransomware listings in numbers like Romania's and Greece's, long-lived espionage access in document and mail systems, and recurring fraud in official names. We have no comparable time series to say whether any of them is growing. Change the plan when the evidence below changes, not on a calendar.

11.1 Key judgements

Judgement	Confidence	Basis and limit
Identity exposure (devices, stealer logs, credential listings) is the most widespread measurable risk to Bulgaria's leading organisations	High for the 250-organisation list	Chapter 3 counts; not national prevalence; signal: new current listings or employee-device associations for your domains
Ransomware groups list Bulgarian organisations in numbers comparable with Romania and Greece	High for observed listings	19 listings in 2026 against 20 and 19; unpublished incidents invisible; signal: Ransompedia listings or a disclosed incident at a Bulgarian organisation
If document-exchange and mail systems lack central logging, plan for long-lived espionage access	Medium (planning assumption)	One officially reported multi-year intrusion; entry route not public; signal: further official disclosures or vendor reports
Plan for further offers of Bulgarian identity data, including national personal numbers	Medium (planning assumption)	Insurance-data offers and confirmed breach notifications from three insurance companies in two groups in 2026; authenticity of the offers unverified; signal: new offers in monitored channels
Plan for recurring fraud waves in the name of the police, the transport ministry and couriers, and for lures tied to public changes such as the euro changeover	Medium (planning assumption)	Repeated official warnings in May, August and November; signal: new look-alike domains and CERT warnings

11.2 What would change the assessment

Current interpretation	Evidence that would change it	Decision affected
Ransomware listings are claims	A disclosed ransomware incident at a Bulgarian essential entity	Raise ransomware readiness; run the restore test in §12.1 first
Insurance-data offers are unverified	A sample matched to a specific system's schema; records confirmed by the data holder; or a regulator's finding	A schema match triggers investigation and a privacy and legal assessment; confirmed records or a regulator's finding trigger the notification decision and customer protection

Current interpretation	Evidence that would change it	Decision affected
The state-network intrusion is unattributed	An official or vendor attribution with indicators	Load the indicators; hunt in document-exchange and mail systems
Current listings mean "validate", not "breached"	Validation shows active accounts without MFA among listed credentials	Escalate to incident response and enforce MFA for the affected population
Hacktivist claims against Bulgaria are few	A sustained DDoS campaign against citizen-facing portals, confirmed by the affected organisation	Revisit upstream mitigation capacity and service-continuity plans

11.3 Conditional scenarios

- **If** a national event, a fine campaign or a payment change is announced, **then** plan for SMS and e-mail phishing in the institution's name (a planning assumption). **Signal:** new look-alike domains and CERT warnings. **Decision:** publish a customer warning and request domain take-downs.
- **If** a new critical vulnerability in an internet-facing mail, VPN or firewall product is disclosed, **then** plan for exploitation attempts at government, energy and telecom organisations; **signal:** CERT Bulgaria and vendor advisories. **Decision:** patch-and-verify within your deadline for internet-facing systems, then hunt for web shells and new administrator accounts.
- **If** card-checker activity on your BIN ranges rises and investigation confirms that specific cards are being tested, **then** plan for card-not-present fraud attempts on those cards; **signal:** clustered low-value declines from foreign gateways. **Decision:** investigate the attempts, check authorisation and fraud signals, and reissue the cards confirmed at risk.

KEY TAKEAWAYS

01

Plan for evidence types, not a new threat: identity exposure, extortion listings, long-lived espionage access and recurring fraud in official names.

02

Each judgement has a signal; change the plan when the signal changes.

03

No comparable time series exists yet to say whether any of these is growing.

CHAPTER 12

Action plan

THIS CHAPTER ANSWERS

What should each team do in the next 90 days, and how will the board know it was done?

20
actions with an owner and completion evidence

INSIDE THIS CHAPTER

12.1 30/60/90 days | 12.2 By role | 12.3 How Brandefense can help

IN SHORT

Start by confirming you receive listing and device alerts, then act on the evidence that is specific to you: current credential listings and employee-device associations. Patch internet-facing mail and edge systems as baseline hygiene. Then close the reporting, phishing, payment-change and mail-authentication gaps, and rehearse a ransomware listing and an identity-data claim. The board knows the work is done from each row's completion evidence and the scorecard below; report both by day 90.

12.1 30/60/90 days

This is a sequence, not a waiting period. A current material threat should enter your incident process immediately.

1 Days 1-30

Confirm that you receive credential-listing and infected-device alerts for your primary domains; if not, arrange them, and record the listing-validation and employee-device rows as blocked until alerts arrive

OWNER
CISO and threat intelligence

COMPLETION EVIDENCE
Alert source named; first alert received

For every current credential listing tied to your domains, validate the account and its MFA status within 5 working days

OWNER
Identity team

COMPLETION EVIDENCE
Each listing has a disposition: reset, already remediated, or not ours, with a date

Validate employee-classified device associations; revoke sessions and tokens where active

OWNER
Identity and endpoint teams

COMPLETION EVIDENCE
Device list reconciled with asset inventory; revocations logged

2 Days 31-60

Turn on central logging for document-exchange, mail and identity systems, and keep it long enough to look back months, not days (§7.2)

OWNER
SOC and infrastructure

COMPLETION EVIDENCE
Log sources and retention recorded; one look-back hunt run

Where DMARC is p=none, missing or invalid, inventory senders and stage enforcement

OWNER
Messaging

COMPLETION EVIDENCE
Aligned senders; p=quarantine with a rollback route

Move mail administrators, privileged and remote users to phishing-resistant MFA (FIDO2 security keys, passkeys or certificate-based sign-in)

OWNER
Identity team

COMPLETION EVIDENCE
Coverage recorded per user group

3 Days 61-90

Take camera, controller and operator-panel management interfaces off the internet; remove default credentials

OWNER
OT and facilities

COMPLETION EVIDENCE
External scan shows no exposed management interfaces

Sign DNS for primary domains where your registrar supports it; fix invalid TLS certificates and add HSTS

OWNER
Network and web teams

COMPLETION EVIDENCE
DNSSEC validation succeeds from an external resolver; certificate checks pass

Run a tabletop combining a ransomware leak-site listing with a simultaneous customer-data claim

OWNER
CISO, communications, legal

COMPLETION EVIDENCE
Decision log and timings, including the 24-hour early warning

Baseline hygiene (§11.3): confirm every internet-facing mail, VPN, firewall and edge server is patched to the vendor's current fixed version, and hunt for web shells and new administrator accounts

OWNER
Infrastructure

COMPLETION EVIDENCE
External re-test passes; hunt completed

Confirm whether you are an essential or important entity, register with the ministry that keeps the register (confirm which with counsel, §10), and name the person who sends the 24-hour early warning

OWNER
CISO and legal

COMPLETION EVIDENCE
Written determination; registration filed, or the date and reason it is pending; named reporter; tested contact route

Name the spokesperson and channel for service-status statements during DDoS and for unverified leak claims

OWNER
Communications and CISO

COMPLETION EVIDENCE
A one-page playbook, approved

Alert on mass mailbox creation and on sign-ins to mail administration from new locations, using the mail platform's admin audit log and the identity provider's sign-in log (Case C)

OWNER
SOC

COMPLETION EVIDENCE
Alert live and tested

Test account-recovery, contact-detail and payee-change processes against an attacker who knows EGN, birth date and address; add step-up checks before loans after a profile change (§8.5)

OWNER
Fraud and customer operations

COMPLETION EVIDENCE
Weaknesses recorded and fixed; retest passed

Require out-of-band confirmation for payment-instruction and payee changes

OWNER
Finance and fraud

COMPLETION EVIDENCE
Procedure signed off; one simulated request caught

Publish customer warnings timed to each SMS-phishing wave in the name of the police, the transport ministry or couriers, and request take-down of look-alike domains

OWNER
Fraud and communications

COMPLETION EVIDENCE
Warnings issued; take-down requests logged

Alert on clustered card-checker declines on your BIN ranges

OWNER
Fraud

COMPLETION EVIDENCE
Alert live; first review recorded

Run a timed restore test of one crown-jewel system

OWNER
Infrastructure

COMPLETION EVIDENCE
Restore time recorded against the recovery time objective (RTO: the longest outage your continuity plan allows)

Contract or test upstream DDoS mitigation for citizen- and customer-facing portals before the next national event

OWNER
Infrastructure and procurement

COMPLETION EVIDENCE
Mitigation test record

Report the scorecard against targets (below)

OWNER
CISO to board

COMPLETION EVIDENCE
Board paper with remaining gaps and owners

Scorecard targets. These are suggested defaults; set your own where policy differs.

Measure	Target
Credential-listing and infected-device monitoring for primary domains, internal or through a provider	In place by day 30
Current listings with a disposition within 5 working days	100% by day 90
Employee-classified devices reconciled with the asset inventory	100% by day 90
Internet-facing mail and edge servers passing an external re-test	100% by day 90
NIS2 status determined and incident reporter named	By day 30
24-hour early-warning route tested, including a weekend	By day 30
Document-exchange, mail and identity logs centralised with look-back retention	By day 60
Primary domains with DMARC at quarantine or reject	100%, or a dated plan, by day 90
Mail administrators, privileged and remote users on phishing-resistant MFA	100%, or a dated plan, by day 90
Payee and contact-detail changes confirmed out of band	100% by day 90
Restore test within RTO	Passed, or a dated fix, by day 90

12.2 By role

Role	First decision
Board	Ask for the current-listing and employee-device numbers for your organisation, the date by which each is validated, and the NIS2 status determination
CISO	Put listing and device monitoring in place first, then validate current listings and employee devices, then central logging; run edge-system patching in parallel as baseline hygiene
SOC	Add detections for web shells on mail and edge servers (web-server and endpoint logs), new administrator accounts (directory change log), mass mailbox creation (mail admin audit log) and sign-ins to administration from new locations (identity-provider sign-in log)
Fraud	Treat EGN, birth date and address as known; add step-up checks after profile changes; monitor clustered card-checker declines on your BINs
Communications	Prepare statements for DDoS, ransomware listings and unverified leak claims that separate claim, verified fact and action

KEY TAKEAWAYS

01

Confirm monitoring, then validate current listings and employee devices, and settle your NIS2 status in the first 30 days.

02

By day 60, turn on central logging, phishing-resistant MFA for mail administrators and out-of-band checks for payment and contact changes.

03

Rehearse a combined ransomware-listing and data-claim scenario, and report the scorecard by day 90.

12.3 How Brandefense can help

Brandefense combines Cyber Threat Intelligence, Digital Risk Protection and External Attack Surface Management. The analysis in this report used the same data that the platform applies to monitored organisations: infected-device and credential associations, current credential-market listings, lookalike domains, exposed documents and dark-web mentions. It does not promise that every claim can be verified or that a historical record remains usable.

Bring your domains, brands and security priorities to a 30-45 minute demo with Sales and Presales. The team can show how platform monitoring relates external signals to the assets you manage. A Brandefense team member or a partner in your region will follow up.

Request a demo

Appendix A. Method

A.1 Window, sources and priority

The research window is 1 January-18 November 2026 by the date a post was published. Own data comes first: Brandefense Blackhole (dark-web and messaging posts, infected-device and credential associations, card material in posts), Ransompedia (ransomware leak-site listings) and Brandefense Atlas exposure ratings. External sources give context and are cited only after the supporting passage was read. Data were extracted on 21 November 2026. Sources S1, S3-S6 and S8 are Brandefense's own data and have no public address. Gaps in the source numbering are intentional, and every external source in Appendix C carries a link and the date we opened it.

A.2 Blackhole posts

Item	Value
Posts tagged as concerning Bulgaria	14,289
Related posts	9,862
Tagged posts after review	7,148-7,529
Bulgaria-specific posts	1,757 in the tagged set; 3,325 in the combined corpus

The counts after review still include some multi-country advertising, so we also report the Bulgaria-specific set, in which Bulgaria is the subject of the post. Both remain upper bounds for criminal activity concerning Bulgaria.

Posts tagged as Bulgarian-language fall sharply from June, and the monthly series are not comparable across mid-2026. We therefore do not compare categories or languages across the year, and we do not read changes from June onwards as trends.

A.3 The 250 organisations

Selection, verification and limits are in §3.1. For each primary domain we report these exposure signals: infected devices, employee devices, credential records, dark-chat and dark-web mentions, new lookalike domains, documents that reference the domain, and current and past credential-market listings. Data were read on 21 November 2026.

A.4 Atlas ratings

Each organisation received an Atlas exposure rating from 0 (no risk observed) to 100. This report publishes only the national headline for the 250 organisations: 50 out of 100. Treat a current credential listing as a reason to validate accounts, not as proof of a breach.

A.5 DNS, TLS and web checks

Results cover mail, SPF, DMARC, DKIM, DNSSEC and CAA (certificate-authority authorisation) records, TLS and the homepage of each domain. Missing, invalid and monitoring-only (p=none) DMARC policies count as no enforcement.

The passive hygiene index is an Odin analytical composite of these email, DNS, TLS and header checks, on a scale of 0-100. A higher value means weaker hygiene; it is a model, not an Atlas rating.

A.6 Card material in posts

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

A.7 Ransomware

We used Ransompedia listings for Bulgaria, Romania, Greece, Serbia and North Macedonia after review, all dates, dated by publication. A public tracker and relayed Blackhole posts are used only as cross-checks.

A.8 Incident coverage

We checked each of the 250 organisations against our data for 1 January–18 November 2026. We also read official news and warning pages month by month for January–November 2026. They include the national CERT, the e-government ministry, the Ministry of Interior, the Prosecutor's Office, the Financial Supervision Commission and the data protection authority. We searched public reporting in English, Bulgarian, Russian and Turkish up to 21 November 2026.

Check for omissions (21 November 2026). An independent check for omissions added two items: a hosting provider's disclosed incident (§7.6) and a vendor report of a hijacked military-sector website (§7.2). We also added an official estimate of payee-IBAN fraud, a caller-ID spoofing warning, a researcher report on local officials' mailboxes and further detail on the July bomb-threat wave. Some government-themed claims could not be corroborated and are not used.

Remaining coverage limits. Our view is partial:

- Some official sites could not be read. The websites of the State Agency for National Security, the Central Election Commission and the National Revenue Agency could not be read; we found their 2026 statements only through press reports.
- Search engines index little of the national news agency's 2026 archive, so its month-by-month coverage remains incomplete.
- Tor ransomware leak sites are covered only through Ransompedia.
- Closed and invite-only forums, private Telegram groups and sales arranged in direct messages are outside our collection.
- Posts deleted before collection are missing.
- Incidents that organisations handle without disclosure stay invisible.

That an incident is absent from this report does not mean it did not happen.

A.9 Confidence and boundaries

High confidence applies to a reproducible measurement, not to a criminal's underlying assertion. Medium indicates an interpretation with a clear supporting line and stated limits. "Unverified" means not independently established; it is neither proof of fabrication nor proof of a breach. Victim organisations are described by role; a state body is named only where an official statement confirms the incident. Actor aliases are printed; links, contacts, indicators and personal data are withheld. Full provenance is held in an internal evidence register.

Appendix B. Evidence register

Selected posts are reproduced as redacted post cards in the chapter shown. Excerpts are short; omissions are marked […]; identifiers, contacts, links and victim organisations are replaced with labels in brackets, under the policy in A.9. Translations are ours. Posting dates are not intrusion dates. Post identifiers, links and full text are held in an internal evidence register.

Card	Posted	Venue	Alias as shown	Language	Shown in
B01	2026-08-30	Lead-trading Telegram channel	Lead-trading channel	English	§4.4
B02	2026-09-10	Cybercrime forum	lauraallen	English, sample in Bulgarian	§4.4

Card	Posted	Venue	Alias as shown	Language	Shown in
B03	2026-08-11	Hacker-news channel relaying a forum thread	Relay channel	English	§4.5
B04	2026-04-05	Cybercrime forum	DuperKinger123	English	§4.5
B05	2026-04-20	Cybercrime forum	thejackal101	English	§4.6
B06	2026-08-08	Cybercrime forum	kookiegst	English	§4.6
B07	2026-02-16	Cracking forum	UHQCombos	English	§4.6
B08	2026-02-18	Breach forum	Jurak	English	§4.6
B09	2026-02-23	Breach forum	Commando	English	§4.6
B10	2026-03-05	Onion-links channel relaying a claim	TheGarudaEye (relayed)	English	§6.2
B11	2026-10-14	Spanish-language relay channel	Z-Alliance / Z-Pentest (relayed)	Spanish	§6.4
B12	2026-08-22	Leak forum	Enigma Group	English	§4.5
B13	2026-04-29	Hacker-forum Telegram chat	wat4ri	English	§4.6
B14	2026-07-12	Telegram registrations and jobs chat	mansorryuwu	English	§8.1
B15	2026-11-05	Cracking forum	annabelle0	English	§8.3
B16	2026-08-23	Leak forum	updap (forum poster)	English	§4.6
B17	2026-01-29	Breach forum	temporary	English, sample in Bulgarian	§4.6
B18	2026-07	Leak-monitor bot relaying a tracker	Leak-monitor bot	English	§7.4

Appendix C. Sources

S1 Brandefense Blackhole posts concerning Bulgaria, post dates 1 January-18 November 2026, extracted 21 November 2026.

S3 Brandefense Blackhole infected-device, breach-database, stealer-log and combolist associations for 250 domains, read 21 November 2026.

S4 Brandefense Atlas exposure ratings and signals for the 250 domains, 21 November 2026, including credential-market listings, lookalike domains, exposed documents and mention statistics.

S5 Brandefense public DNS, TLS and homepage checks of the 250 domains, 21 November 2026.

S6 Brandefense Ransompedia, listings after review for Bulgaria, Romania, Greece, Serbia and North Macedonia, all dates, extracted 21 November 2026.

S7 ransomware.live, public ransomware tracker (country page withheld), accessed 21 November 2026 (cross-check only). https://www.ransomware.live/ (page URL withheld). Verified on 21 November 2026.

S8 Brandefense Blackhole, Bulgaria-associated cards in collected posts (counts only), 21 November 2026.

S14 DataReportal (Kepios), *Digital 2027: Bulgaria*, 5 November 2026 (data for October 2026). https://datareportal.com/reports/digital-2027-bulgaria. Verified on 21 November 2026.

S15 European Central Bank, press release on the euro's entry into circulation in Bulgaria, 1 January 2026. https://www.ecb.europa.eu/press/pr/date/2026/html/ecb.pr260101~c830245e42.en.html. Verified on 21 November 2026.

S16 European Commission, Access2Markets, "Bulgaria adopts euro on 1 January 2026", 28 January 2026. https://trade.ec.europa.eu/access-to-markets/en/news/bulgaria-adopts-euro-1-january-2026. Verified on 21 November 2026.

S17 BNT, "Police issue fraud warning ahead of euro changeover in Bulgaria", 29 December 2025, reporting the Ministry of Interior. https://bntnews.bg/news/police-issue-fraud-warning-ahead-of-euro-changeover-in-bulgaria-1371604news.html. Verified on 21 November 2026.

S18 BTA, "Electronic Governance Ministry: No increased cyber activity on election day", 19 April 2026, 16:12. https://www.bta.bg/en/news/1109158-electronic-governance-ministry-no-increased-cyber-activity-on-election-day. Verified on 21 November 2026.

S19 News.bg, "След кибератака МС и МЕУ останаха без интернет" (After a cyberattack the Council of Ministers and the e-government ministry were left without internet), 19 April 2026, citing Nova. https://news.bg/politics/sled-kiberataka-ms-i-meu-ostanaha-bez-internet.html. Verified on 21 November 2026.

S20 BNR (Radio Bulgaria), "No significant foreign interference found in Bulgaria's parliamentary elections", 5 May 2026. https://bnrnews.bg/en/post/465510/no-significant-foreign-interference-found-in-bulgarias-parliamentary-elections. Verified on 21 November 2026.

S21 BTA, "National Security Agency Issues Cybersecurity Instructions to Strategic Facilities Ahead of Presidential Election", 17 September 2026. https://www.bta.bg/en/news/1206346-national-security-agency-issues-cybersecurity-instructi. Verified on 21 November 2026.

S22 Ministry of Innovation and Digital Transformation, statement of 5 August 2026 on unauthorised access to administrative networks. https://midt.gov.bg/bg/news/1351; English report by BTA, 5 August 2026: https://www.bta.bg/en/news/bulgaria/1180195-government-uncovers-apparent-years-long-breach-of-administrative-networks. Verified on 21 November 2026.

S23 Ministry of Innovation and Digital Transformation, statement of 18 November 2026 on the cyber-espionage operation against the state administration. https://midt.gov.bg/bg/news/1614. Verified on 21 November 2026.

S24 Mediapool, report on the minister's briefing on the five-year intrusion, 18 November 2026. https://www.mediapool.bg/biznes/hakeri-imali-5-godini-dostap-do-darzhavni-mrezhi-iztochili-pone-62-mln-stranitsi-ot-dokumenti/. Verified on 21 November 2026.

S25 Reuters, "Bulgaria uncovers five-year cyberespionage operation", 18 November 2026, as syndicated by Internazionale. https://www.internazionale.it/ultime-notizie-reuters/2026/11/18/bulgaria-uncovers-five-year-cyberespionage-operation. Verified on 21 November 2026.

S26 National Assembly decision of 8 May 2026 creating the Ministry of Innovation and Digital Transformation, State Gazette No. 43 of 12 May 2026, as indexed by LexAlert. https://lexalert.bg/archive/2026/43/2543/; ministry profile: https://midt.gov.bg/bg/about/ministry. Verified on 21 November 2026.

S27 CERT Bulgaria, national computer security incident response team. https://www.govcert.bg/en/. Verified on 21 November 2026.

S28 Act amending and supplementing the Cybersecurity Act, adopted 5 February 2026, State Gazette No. 17 of 13 February 2026 (official text). https://dv.parliament.bg/DVWeb/showMaterialDV.jsp?idMat=241234. Verified on 21 November 2026.

S29 Ministry of Innovation and Digital Transformation, "The European Commission closed infringement procedure No. 2024/0257 against Bulgaria", 1 October 2026. https://midt.gov.bg/bg/news/1561. Verified on 21 November 2026.

S30 BNT, "Cyberattacks on Bulgaria on the rise", 16 March 2026, quoting the cybersecurity manager of Information Services. https://bntnews.bg/news/cyberattacks-on-bulgaria-on-the-rise-1383934news.html. Verified on 21 November 2026.

S31 State Agency for National Security, report on activities in 2025, dated 21 April 2026, published by the Council of Ministers. https://www.gov.bg/files/common/DANS%202025.docx. Verified on 21 November 2026.

S32 DiarioBitcoin, report on a forum offer of 3.1 million records attributed to an insurer (title names the company), 10 September 2026. https://www.diariobitcoin.com/ (article URL withheld). Verified on 21 November 2026.

S34 e-security.bg, report on the data protection authority's confirmation of breach notifications by three insurance companies in two groups (title names the companies), 26 September 2026, citing BIRD.BG. https://e-security.bg/ (article URL withheld). Verified on 21 November 2026.

S35 CERT Bulgaria, warning on bomb-threat e-mails sent to state institutions from hijacked accounts, 9 July 2026. https://www.govcert.bg/warnings/%d0%ba%d0%b0%d0%bc%d0%bf%d0%b0%d0%bd%d0%b8%d1%8f-%d1%81%d1%8a%d1%81-%d0%b7%d0%b0%d0%bf%d0%bb%d0%b0%d1%88%d0%b8%d1%82%d0%b5%d0%bb%d0%bd%d0%b8-%d0%b8%d0%bc%d0%b5%d0%b9%d0%bb-%d1%81%d1%8a%d0%be%d0%b1/. Verified on 21 November 2026.

S37 CERT Bulgaria, warning on attacks against internet-exposed commercial refrigeration controllers, 6 November 2026. https://www.govcert.bg/warnings/%d0%ba%d0%b8%d0%b1%d0%b5%d1%80%d0%b0%d1%82%d0%b0%d0%ba%d0%b8-%d1%81%d1%80%d0%b5%d1%89%d1%83-%d1%82%d1%8a%d1%80%d0%b3%d0%be%d0%b2%d1%81%d0%ba%d0%b8-%d1%85%d0%bb%d0%b0%d0%b4%d0%b8%d0%bb%d0%bd%d0%b8/. Verified on 21 November 2026.

S38 Ministry of Interior, statement of the minister on cybercrime and the Cybercrime Directorate, 20 July 2026. https://www.mvr.bg/press/%D0%B0%D0%BA%D1%82%D1%83%D0%B0%D0%BB%D0%BD%D0%B0-%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F/%D0%B0%D0%BA%D1%82%D1%83%D0%B0%D0%BB%D0%BD%D0%B0-%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F/%D0%BD%D0%BE%D0%B2%D0%B8%D0%BD%D0%B8/92003. Verified on 21 November 2026.

S39 Ministry of Interior, arrest of two suspects linked to "Smishing Triad", 18 March 2026. https://www.mvr.bg/press/%D0%B0%D0%BA%D1%82%D1%83%D0%B0%D0%BB%D0%BD%D0%B0-%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F/%D0%B0%D0%BA%D1%82%D1%83%D0%B0%D0%BB%D0%BD%D0%B0-%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F/%D0%BD%D0%BE%D0%B2%D0%B8%D0%BD%D0%B8/89345. Verified on 21 November 2026.

S40 Ministry of Interior, warning on scams against sellers on classified-ad sites, 23 January 2026. https://www.mvr.bg/press/%D0%B0%D0%BA%D1%82%D1%83%D0%B0%D0%BB%D0%BD%D0%B0-%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F/%D0%B0%D0%BA%D1%82%D1%83%D0%B0%D0%BB%D0%BD%D0%B0-%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F/%D0%BD%D0%BE%D0%B2%D0%B8%D0%BD%D0%B8/88502. Verified on 21 November 2026.

S41 Ministry of Interior, "Tens of thousands of phishing messages were sent to users in the name of institutions and courier companies", 11 May 2026. https://www.mvr.bg/press/%D0%B0%D0%BA%D1%82%D1%83%D0%B0%D0%BB%D0%BD%D0%B0-%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F/%D0%B0%D0%BA%D1%82%D1%83%D0%B0%D0%BB%D0%BD%D0%B0-%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F/%D0%BD%D0%BE%D0%B2%D0%B8%D0%BD%D0%B8/90489. Verified on 21 November 2026.

S42 Prosecutor's Office, Sofia City Prosecutor's Office charges a person with computer crimes, 30 October 2026. https://prb.bg/bg/news/80130-sofiyska-gradska-prokuratura-privleche-obvinyaem-za-kompyutarni-prestapleniya. Verified on 21 November 2026.

S43 Ministry of Interior, participation in Operation Endgame, 13 November 2026. https://www.mvr.bg/press/%D0%B0%D0%BA%D1%82%D1%83%D0%B0%D0%BB%D0%BD%D0%B0-%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F/%D0%B0%D0%BA%D1%82%D1%83%D0%B0%D0%BB%D0%BD%D0%B0-%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F/%D0%BD%D0%BE%D0%B2%D0%B8%D0%BD%D0%B8/94424. Verified on 21 November 2026.

S44 Ministry of Interior, Plovdiv police seizure of a computer holding scanned identity cards, 2 April 2026. https://www.mvr.bg/press/%D0%B0%D0%BA%D1%82%D1%83%D0%B0%D0%BB%D0%BD%D0%B0-%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F/%D0%B0%D0%BA%D1%82%D1%83%D0%B0%D0%BB%D0%BD%D0%B0-%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F/%D0%BD%D0%BE%D0%B2%D0%B8%D0%BD%D0%B8/89768. Verified on 21 November 2026.

S45 Financial Supervision Commission, warning on fake e-mails in its name, 7 January 2026. https://www.fsc.bg/falshivi-imejli-mamyat-ot-imeto-na-kfn/. Verified on 21 November 2026.

S46 Financial Supervision Commission, warning on the theft of crypto-asset companies through forged register entries, 3 February 2026. https://www.fsc.bg/kfn-preduprezhdava-za-krazhbi-na-kriptokompanii/. Verified on 21 November 2026.

S47 Ministry of Interior, warning on SMS and app messages about speeding fines, 8 May 2026. https://www.mvr.bg/press/%D0%B0%D0%BA%D1%82%D1%83%D0%B0%D0%BB%D0%BD%D0%B0-%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F/%D0%B0%D0%BA%D1%82%D1%83%D0%B0%D0%BB%D0%BD%D0%B0-%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F/%D0%BD%D0%BE%D0%B2%D0%B8%D0%BD%D0%B8/90448. Verified on 21 November 2026.

S48 CERT Bulgaria, warning on an ongoing SMS phishing campaign impersonating the police, the traffic police and the transport ministry, 18 May 2026. https://www.govcert.bg/warnings/%d0%bf%d1%80%d0%be%d0%b4%d1%8a%d0%bb%d0%b6%d0%b0%d0%b2%d0%b0%d1%89%d0%b0-phishing-%d0%ba%d0%b0%d0%bc%d0%bf%d0%b0%d0%bd%d0%b8%d1%8f-%d0%bf%d1%80%d0%b5%d0%b4%d1%81%d1%82%d0%b0%d0%b2%d1%8f%d1%89%d0%b0/. Verified on 21 November 2026.

S49 CERT Bulgaria, warning on SMS phishing about electronic fines, 11 November 2026. https://www.govcert.bg/warnings/phishing-november-2026/. Verified on 21 November 2026.

S50 Ministry of Interior, closure of a Sofia call centre running investment fraud, published 10 June 2026; the release body dates the operation 4 July 2026, so the operation date is unresolved. https://www.mvr.bg/press/%D0%B0%D0%BA%D1%82%D1%83%D0%B0%D0%BB%D0%BD%D0%B0-%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F/%D0%B0%D0%BA%D1%82%D1%83%D0%B0%D0%BB%D0%BD%D0%B0-%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F/%D0%BD%D0%BE%D0%B2%D0%B8%D0%BD%D0%B8/91191. Verified on 21 November 2026.

S51 Ministry of Interior, closure of four call centres running AI-generated crypto-investment fraud, 21 October 2026. https://www.mvr.bg/press/%D0%B0%D0%BA%D1%82%D1%83%D0%B0%D0%BB%D0%BD%D0%B0-%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F/%D0%B0%D0%BA%D1%82%D1%83%D0%B0%D0%BB%D0%BD%D0%B0-%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F/%D0%BD%D0%BE%D0%B2%D0%B8%D0%BD%D0%B8/93747. Verified on 21 November 2026.

S52 Prosecutor's Office, detention for computer fraud involving a changed bank profile and an online loan, 19 June 2026. https://prb.bg/bg/news/78652-po-iskane-na-sofiyska-rayonna-prokuratura-sadat-zadarzha-mazh-za-kompyutarna-izm. Verified on 21 November 2026.

S53 Ministry of Interior, warning on fake "police summons" e-mails, 28 August 2026. https://www.mvr.bg/press/%D0%B0%D0%BA%D1%82%D1%83%D0%B0%D0%BB%D0%BD%D0%B0-%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F/%D0%B0%D0%BA%D1%82%D1%83%D0%B0%D0%BB%D0%BD%D0%B0-%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F/%D0%BD%D0%BE%D0%B2%D0%B8%D0%BD%D0%B8/92611. Verified on 21 November 2026.

S54 Ministry of Interior, cybercrime officers' talk on hijacked accounts, 19 November 2026. https://www.mvr.bg/press/%D0%B0%D0%BA%D1%82%D1%83%D0%B0%D0%BB%D0%BD%D0%B0-%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F/%D0%B0%D0%BA%D1%82%D1%83%D0%B0%D0%BB%D0%BD%D0%B0-%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F/%D0%BD%D0%BE%D0%B2%D0%B8%D0%BD%D0%B8/94537. Verified on 21 November 2026.

S56 Ministry of Interior, participation in Operation PowerOFF against DDoS-for-hire services, 16 April 2026. https://www.mvr.bg/press/%D0%B0%D0%BA%D1%82%D1%83%D0%B0%D0%BB%D0%BD%D0%B0-%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F/%D0%B0%D0%BA%D1%82%D1%83%D0%B0%D0%BB%D0%BD%D0%B0-%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F/%D0%BD%D0%BE%D0%B2%D0%B8%D0%BD%D0%B8/90027. Verified on 21 November 2026.

S58 CMS, "EU DORA Regulation amendments submitted to Bulgarian Parliament", 7 February 2025 (updated 24 September 2026). https://cms.law/en/bgr/legal-updates/eu-dora-regulation-amendments-submitted-to-bulgarian-parliament. Verified on 21 November 2026.

S59 Council of Ministers public-consultation portal, draft Act on the Resilience of Critical Entities, consultation 27 May–26 June 2025. https://www.strategy.bg/bg/public-consultations/11134. Verified on 21 November 2026.

S60 Ministry of Innovation and Digital Transformation, Council of Ministers decision on the administrations to be included in the National Cybersecurity System, 4 November 2026. https://midt.gov.bg/bg/news/1604. Verified on 21 November 2026.

S61 BTA, "Hacker attacks on government websites continue", statement of the Minister of Innovation and Digital Transformation, 19 November 2026. https://www.bta.bg/en/news/bulgaria/1250121-hacker-attacks-on-government-websites-continue-innovation-and-digital-transform. Verified on 21 November 2026.

S62 Fakti, citing BNR, statement of the head of the cyber-intelligence department of the police organised-crime directorate on payee-IBAN fraud against companies, 3 June 2026. https://www.fakti.bg/en/bulgaria/1058695-gdbop-hakeri-iztochvat-milioni-ot-firmi-v-balgaria. Verified on 21 November 2026.

S63 BTA, "Regulator, mobile operators take aim at surge in caller ID spoofing scams", 14 August 2026. https://www.bta.bg/en/news/1185761-regulator-mobile-operators-take-aim-at-surge-in-caller-id-spoofing-scams. Verified on 21 November 2026.

S64 ENISA, *ENISA Threat Landscape* 2026, September 2026. https://www.enisa.europa.eu/sites/default/files/2026-09/ENISA%20Threat%20Landscape%202026_Final.pdf. Verified on 21 November 2026.

S65 Money.bg, report on unauthorised access to the internal system of a hosting provider (title names the company), 17 November 2026 (updated 18 November). https://money.bg/ (article URL withheld). Verified on 21 November 2026.

S66 Sekoia, "Poisoned Source: APT29 watering holes target mobile devices with n-day exploits", 4 November 2026. https://www.sekoia.com/blog/poisoned-source-apt29-watering-holes-targets-mobile-devices-with-n-day-exploits; reported in Bulgarian by Ruse.news, 5 November 2026: https://ruse.news/index.php/2026/11/05/kampaniya-za-kiberataki-vklyuchila-balgarski-sajt-ot-voennata-sfera/. Verified on 21 November 2026.

S67 Fakti, republishing Reuters, report on an e-mail campaign that researchers attributed to APT28, which reached mailboxes of local officials in the Plovdiv region, 15 April 2026. https://www.fakti.bg/ (article URL withheld). Verified on 21 November 2026.

S68 CISA, FBI and international partners, joint advisory AA25-343A, "Pro-Russia Hacktivists Conduct Opportunistic Attacks Against US and Global Critical Infrastructure", 9 December 2025; NCSC New Zealand republication, 15 December 2025. https://www.ncsc.govt.nz/alerts/pro-russia-hacktivists-conduct-attacks-against-critical-infrastructure. Verified on 21 November 2026.

S69 KELA, "OT threat intelligence, part 2", updated 3 September 2026. https://www.kelacyber.com/blog/ot-threat-intelligence-part2/. Verified on 21 November 2026.

S70 Cyble, Krybit ransomware threat-actor profile, 22 September 2026. https://cyble.com/threat-actor-profiles/krybit-ransomware-threat-actor/. Verified on 21 November 2026.

S72 BNR (Radio Bulgaria), "Wave of bomb threats paralyzes dozens of institutions across Bulgaria", 7 July 2026. https://bnrnews.bg/en/post/499930/wave-of-bomb-threats-paralyzes-dozens-of-institutions-across-bulgaria. Verified on 21 November 2026.

S73 Financial Supervision Commission, English text of the Markets in Crypto-Assets Act, State Gazette No. 54 of 4 July 2025. Its final provisions amend the Credit Institutions Act, the Payment Services and Payment Systems Act (new Art. 182b) and the Financial Supervision Commission Act for DORA. https://www.fsc.bg/wp-content/uploads/2026/01/markets_in_cryptoassets_act.pdf. Verified on 21 November 2026.

Appendix D. Glossary

- **Blackhole:** Brandefense's cybercrime data source covering posts, infected devices, credentials and card material.
- **Ransompedia:** Brandefense's ransomware database; listings record criminal claims.
- **Atlas:** Brandefense's external exposure scoring; scores run from 0 (nothing observed) to 100.
- **Infected device:** a device whose stealer log contains a login to the organisation's domain; "employee" is a classification, not verified employment.
- **Credential-market listing:** a credential tied to the domain offered on a monitored market at the time of the check.
- **Combolist:** a list of login and password pairs assembled from various sources; age and validity vary.
- **Stealer log:** data captured by information-stealing malware from a device.
- **Checker bot:** a bot that tests stolen cards against payment gateways and prints the result.
- **Post card:** a redacted reproduction of one dark-web post, with venue, date, alias, language and what it does and does not establish.
- **Relay:** a third-party channel or bot that reposts another actor's claim; a relay is weaker evidence than the actor's own post.
- **Bulgaria-specific post:** a post in which Bulgaria is the subject, not one entry on a multi-country list.
- **EGN:** the Bulgarian personal identification number (**единен граждански номер**), assigned to every citizen.
- **IBAN:** International Bank Account Number; Bulgarian IBANs begin with BG.
- **NIS2:** the EU directive on a high common level of cybersecurity (Directive (EU) 2022/2555), transposed in Bulgaria through the 2026 amendments to the Cybersecurity Act.
- **Essential and important entities:** the two NIS2 categories of covered organisations; essential entities face the higher fine ceiling.
- **Early warning:** the first NIS2 incident report, due within 24 hours of detecting a significant incident.
- **DORA:** the EU Digital Operational Resilience Act for financial entities.
- **CSIRT:** computer security incident response team; CERT Bulgaria is the national one.
- **DMARC / SPF / DKIM:** email-authentication standards; DMARC tells receivers what to do with mail that fails.
- **DNSSEC:** signatures that let resolvers verify DNS answers.
- **DS record:** the record in the parent zone that links a domain to its DNSSEC keys.
- **HSTS:** a web header telling browsers to use HTTPS only.
- **TLP:CLEAR:** may be shared without restriction; other legal duties still apply.
- **BIN:** the issuer's card-number prefix (bank identification number).
- **KYC:** "know your customer" identity checks at banks, exchanges and other services.
- **Drops and mule accounts:** people, and accounts opened in their names, used to receive and move fraud proceeds.
- **Smishing:** phishing by SMS or messaging app.
- **Look-alike domain:** a domain registered to resemble a real organisation's, used for phishing.
- **MFA (multi-factor authentication):** a sign-in that needs a second factor beyond the password.
- **Phishing-resistant MFA:** sign-in tied to the real site (FIDO2 security keys, passkeys or certificates), so a relay page cannot reuse it.
- **OT:** operational technology, the systems that run physical processes; an operator panel is its local control screen.
- **Web shell:** a script placed on a web server that gives an attacker remote control of it.
- **Headline score:** the national Atlas figure for all 250 organisations (50 out of 100; higher means more exposure).
- **p=none:** a DMARC policy that only monitors and does not ask receivers to reject or quarantine.

- **Passive hygiene index:** an Odin analytical composite of email, DNS, TLS and header checks; 0-100, higher means weaker.
- **RTO:** recovery time objective, the longest outage a continuity plan allows.
- **3-D Secure:** the one-time code or app approval a card issuer asks for during an online card payment.
- **SCADA:** supervisory control and data acquisition, software that monitors and controls industrial processes; Rapid SCADA is one open-source product.
- **VNC:** a remote-desktop protocol; exposed VNC connections give remote control of a screen.
- **SSRF:** server-side request forgery, a flaw that makes a server send requests on an attacker's behalf.
- **CAA record:** a DNS record that names which certificate authorities may issue certificates for a domain.
- **CMS:** content-management system, the software that runs a website.
- **APT28 / APT29:** names that security vendors use for two espionage groups; the attribution in each case is the source's, not ours.
- **Lead base:** a list of personal contact records sold for marketing or fraud.

About this report

Prepared by Odin by Brandefense. Version 1.0 was completed on 21 November 2026.

Research cutoff: 18 November 2026 (primary data window); official and press reporting was read up to 21 November 2026 (Appendix A.8). The report prioritises Brandefense's own data, keeps criminal claims separate from independently established incidents and does not claim a complete census of cybercrime affecting Bulgaria. Recommendations describe what organisations could do; they do not state that any organisation has or has not done them. The authors take no position on Bulgarian or international politics; official statements and attributions are reported as the source gave them. A Bulgarian-language edition accompanies this report; where the two differ, the English edition prevails.

© 2026 Brandefense. All rights reserved.