ДОКЛАД ЗА ДЪРЖАВА · BRANDEFENSE COUNTRY REPORT · BULGARIA 2026 · TLP:CLEAR · 95 МИН ЧЕТЕНЕ

Brandefense Доклад за киберзаплахите в България 2026

Изложеност на идентичността, обяви за изнудване и многогодишно проникване в държавни мрежи в нов член на еврозоната

TRANSLATED WITH AI

Това издание е преведено с помощта на изкуствен интелект от оригиналния английски текст; английската версия е водеща.

АВТОР
Odin by Brandefense

ПУБЛИКУВАН
21 ноември 2026

ВРЕМЕ ЗА ЧЕТЕНЕ
95 мин четене

ИЗДАНИЕ
Версия 1.0 · Public Research Edition · TLP:CLEAR

ИЗСЛЕДВАН ПЕРИОД
1 януари–18 ноември 2026

96 от 250
организации имаха идентификационни данни, обявени за продажба в деня на проверката

1 757
уникални публикации в маркирания набор, които се отнасят конкретно до България

19
вписвания на рансъмуер групи в сайтове за изтичане за България през 2026 г. след преглед, назоваващи 17 организации

110 USD
медианна искана цена за банков или платежен акаунт в прегледаните публикации

СЪДЪРЖАНИЕ

01 Резюме за ръководството
02 Цифровият контекст и контекстът на сигурността в България
04 Какво виждаме в тъмната мрежа
06 Хактивизъм, DDoS и твърдения за смущения
08 Икономиката на измамите
10 Регулаторна рамка и национален отговор
12 План за действие
B Приложение B. Регистър на доказателствата
D Приложение D. Речник
Карта на доклада
03 Национална експозиция: 250 водещи организации
05 Примери за насочване по сектори
07 Участници на заплахи
09 Банки и финанси: задълбочен анализ
11 Перспективи
A Приложение A. Метод
C Приложение C. Източници
За този доклад

ГЛАВА 1

Резюме за ръководството

ТАЗИ ГЛАВА ОТГОВАРЯ НА ВЪПРОСА

Какво се случи през 2026 г., кое е най-важно за българските организации и какво трябва да решат първо ръководителите?

4

решения за ръководителите, всяко обвързано с доказателства от главите

В ТАЗИ ГЛАВА

Четири решения за ръководителите | Годината в числа

НАКРАТКО

За 250-те водещи български организации, които оценихме, основната измерена експозиция е свързана с идентичността: асоциации със заразени устройства и идентификационни данни, както и идентификационни данни, обявени за продажба. Най-сериозното съобщено проникване е петгодишна шпионска операция в държавните мрежи за обмен на документи, разкрита от правителството. Рансъмуер групи обявиха 17 български организации, а продавачи рекламираха данни на застрахователни клиенти. Действайте в този ред: проверете обявите за вашите идентификационни данни, централизирайте логовете на пощата и системите за документи, след това упражнете сценарий с обява за изнудване.

Този доклад съчетава три собствени източника на данни на Brandefense с проверени публични съобщения. **Brandefense Blackhole** предостави 14 289 публикации, маркирани като отнасящи се до България, и още 9 862 свързани публикации. Той предостави и записи за заразени устройства и идентификационни данни за 250 избрани организации, както и картови данни, появили се в явен текст в публикации. **Ransompedia** предостави обяви от сайтове за изтичане на рансъмуер групи за България и четири регионални държави за сравнение. Оценките за експозиция на **Atlas** бяха изчислени за 250-те организации. Това са отделни съвкупности и никога не се събират.

Националната обобщаваща оценка на Atlas за 250-те организации е 50 от 100, където 0 означава, че не е наблюдаван риск, а по-високите стойности означават по-голяма експозиция.

1. **Експозицията на идентичността е широко разпространена; обявите за идентификационни данни са на първо място.** От 250-те организации 218 имат заразени устройства, свързани с домейните им (общо 301 070, долна граница), а 241 имат исторически записи за идентификационни данни. Два потребителски доставчика на уебпоща държат 99,3% от 76,7 милиона записа, защото домейните им са пощенските адреси на потребителите. Останалите 248 организации държат 565 935. Това са кумулативни бройки на асоциации, налични към 21 ноември 2026 г., независимо от датата на прихващане. Те могат да засягат служители, студенти или клиенти, а дали някое влизане все още работи, изисква проверка. [S1][S3]

96 от 250 организации имаха идентификационни данни, обявени за продажба към момента на проверката. Третирайте обявата като повод да проверите акаунтите, а не като доказателство за пробив: тя не показва колко акаунта са засегнати, нито чии са. [S4]

2. **Правителството съобщава за петгодишно проникване в държавни мрежи.** През август Министерството на иновациите и дигиталната трансформация разкри неоторизиран достъп до административни мрежи. През ноември то заяви, че достъпът е продължавал от 2021 г. през инфраструктурата, която институциите използват за обмен на документи. Министърът определи обема на поне 130 GB, над 62 милиона страници. По думите му се смята, че са замесени няколко международни групи, без категорична връзка с държава. Досегашните проверки не са открили изтичане на лични данни на граждани. Нищо в нашите данни от тъмната мрежа не може да бъде свързано с това. [S22][S23][S24][S25]

3. **Рансъмуер групите публикуваха почти толкова български обяви, колкото румънски и гръцки.** След преглед Ransompedia съдържа 19 български обяви с дати 1 януари–18 ноември 2026 г. (17 организации), срещу 7 обяви за цялата 2025 г. Румъния има 20, а Гърция 19 за същия период. Сред обявените организации са холдингово дружество и застрахователното му дъщерно дружество,

търговско дружество, аптечна верига и компания за интернет услуги. Доколкото открихме, нито една не беше потвърдила инцидент към нашата крайна дата. [S6]

4. Данните на застрахователни клиенти с ЕГН бяха най-значимото твърдение за данни през годината. Между 30 август и 16 септември поне три оферти рекламираха данни на български застрахователни клиенти с единни граждански номера (ЕГН), като една твърдеше „2.2M+" записа. Комисията за защита на личните данни (КЗЛД) потвърди уведомления за нарушение от три застрахователни дружества от две групи, без да потвърди обемите. Един застраховател отрече проникване в собствените си системи. Какъвто и да е произходът, ЕГН, датата на раждане и адресът трябва да се третират като известни на престъпниците. [S1][S32][S34]

5. Измамите използват официални имена; един срив в изборния ден остава необяснен. Полицията и CERT България съобщиха за SMS фишинг от името на полицията, транспортното министерство и куриерски фирми, както и за кол центрове, които извършват инвестиционни измами. Според полицията три до четири фирми седмично губят пари от измами с подменен IBAN на получателя. В деня на изборите през април два държавни сайта според съобщенията са били недостъпни в продължение на часове. В същото време министерството заяви, че системите му работят нормално. Хактивистките твърдения срещу България бяха малко в нашите данни и нито едно не беше потвърдено. [S19][S41][S48][S51][S62]

Четири решения за ръководителите

1. **Третирайте актуалните обяви за идентификационни данни като повод за инцидент, а не като статистика.** Насочвайте всяка актуална обява на пазара, свързана с вашите домейни, към екипа по идентичност и документирайте решение по нея в рамките на 5 работни дни. Ескалирайте към екипа за реагиране при инциденти, ако бъде открит активен акаунт без многофакторно удостоверяване (MFA). Осигурете наблюдение на обявите за идентификационни данни и на заразените устройства за вашите домейни от ден 1, чрез вътрешен екип или доставчик (§12.1).
2. **Централизирайте логовете за поща, идентичност и обмен на документи и търсете назад във времето.** Според министерството проникването в държавните мрежи е останало скрито около пет години и е открито при внедряването на национална система за наблюдение (§7.2). Пазете логовете достатъчно дълго, за да можете да търсите месеци назад, и настройте сигнали при нови администраторски акаунти и влизания в администрирането на пощата.
3. **Изяснете статуса си по NIS2 и упражнете 24-часовото докладване.** Измененият Закон за киберсигурност изисква ранно предупреждение в рамките на 24 часа от значителен инцидент, с глоби до 10 милиона EUR или 2% от оборота (§10). Определете още сега кой докладва и упражнете докладването заедно със сценарий за обява в сайт за изтичане на рансъмуер група.
4. **Свържете екипите по идентичност, измами и операции по сигурността около данните на гражданите.** Офертите за застрахователни данни и документи за самоличност не разкриват пробита система, но захранват измами с представяне за друго лице и с възстановяване на акаунти. Тествайте процесите за промяна на данни за контакт, получатели на плащания и кредити срещу нападател, който знае ЕГН, датата на раждане и адреса.

Годината в числа

19 / 17

Рансъмуер обяви за България в Ransompedia след преглед, с дати 1 януари–18 ноември 2026 г. / организации, които те назовават (7 обяви за цялата 2025 г.)

КАКВО НЕ Е

Не са потвърдени пробиви; необявените и непубликуваните случаи остават невидими

14 289

Публикации в Blackhole, маркирани като отнасящи се до България, 1 януари–18 ноември 2026 г.

КАКВО НЕ Е

Не е брой атаки; повечето са реклама за много държави

1 757

уникални маркирани публикации, в които България е темата

КАКВО НЕ Е

Не са уникални инциденти; бройките са горна граница

>130 GB

документи, за които министърът заяви, че са изтеглени от държавни мрежи от 2021 г. насам

КАКВО НЕ Е

Не са приписани на държава; според досегашните проверки не са лични данни на граждани

250

водещи публични и частни организации, оценени с Brandefense Atlas

КАКВО НЕ Е

Не е случайна извадка; не е оценка за разпространението в страната

301 070

заразени устройства, свързани с тези 250 домейна (8 860 класифицирани като на служители, без двата доставчика на уебпоща); кумулативно, всички записи, налични към 21 ноември 2026 г.

КАКВО НЕ Е

Не само за 2026 г., не са уникални хора, не са проверени актуални заразявания; долна граница

565 935

исторически записи за идентификационни данни за 248-те домейна без двата потребителски доставчика на уебпоща (76,7 милиона с тях)

КАКВО НЕ Е

Не само за 2026 г.; не са уникални акаунти или активни пароли

96 от 250

организации с идентификационни данни, обявени за продажба към момента на проверката

КАКВО НЕ Е

Не е брой акаунти или потвърдени пробиви

126

уникални платежни карти, свързани с България, видени в явен текст в събрани публикации от тъмната мрежа (81 приписани на посочен издател, 45 обозначени само като български)

КАКВО НЕ Е

Не е стойност на загуби от измами; тесен обхват (§8.2)

59%

от 250-те организации налагат DMARC (148)

КАКВО НЕ Е

Не е мярка за успеха на фишинга или за сигурността на доставката

Карта на доклада

Дванадесет глави, пет пътя за четене. Започнете от реда, който съответства на вашата роля; всяка глава започва с въпроса, на който отговаря, а глави 2–12 завършват с три основни извода.

Съвет на директорите и ръководство
Какво се случи, колко сме изложени и какво трябва да решим?
КЪМ 1 3 12

CISO и ръководители по сигурността
Кои излагания са наши, кои извършители имат значение и кои контроли са първи?
КЪМ 3 7 9 10 12

SOC и разузнаване на заплахи
Какво публикуваха извършителите, как са свързани и какво показа проникването в държавните мрежи?
КЪМ 4 6 7 12 Прил. A-B

Измами и защита на клиентите
Как се търгуват български самоличности, акаунти и карти и къде го виждат банките?
КЪМ 4 5 8 9

Комуникации и правен отдел
Как да говорим за непроверени твърдения и какво изисква измененият Закон за киберсигурност?
КЪМ 6 10 12

01 **Резюме за ръководството**
Какво се случи през 2026 и какво трябва да решат ръководителите първо

02 **Контекст**
Кои особености на България оформят заплахите

03 **Национално излагане**
Колко изложени са 250 водещи организации

04 **Тъмна мрежа**
Какво публикуват престъпниците конкретно за България

05 **Сектори**
Кои сектори се споменават и какъв отговор изисква всеки

06 **Хактивизъм**
Какво беше заявено, какво беше потвърдено, как да се подготвим

07 **Участници на заплахи**
Кои са извършителите, как са свързани, какво показват официалните данни

08 **Икономика на измамите**
Как самоличностите и акаунтите се превръщат в пари

09 **Банков сектор**
Къде се намира видимото излагане на банките

10 **Регулаторна рамка**
Какво изискват сега измененията по NIS2

11 **Перспективи**
За какво да се планира и какво би променило плана

12 **План за действие**
Кой какво прави в рамките на 90 дни

ГЛАВА 2

Цифровият контекст и контекстът на сигурността в България

02

ТАЗИ ГЛАВА ОТГОВАРЯ НА ВЪПРОСА

Кои особености на България определят заплахите в този доклад и кои официални изявления задават рамката за 2026 г.?

89,8%

проникване на интернет, при 9,26 милиона мобилни връзки

В ТАЗИ ГЛАВА

2.1 Свързано население със силен мобилен навик
2.2 Преминаването към еврото като примамка за измами
2.3 Изборите и защитата на държавните системи
2.4 Дългогодишен неоторизиран достъп до държавни мрежи
2.5 Ново министерство и нов закон за киберсигурността

НАКРАТКО

Четири фактора определят картината на заплахите в България през 2026 г. Преминаването към еврото даде на измамниците нова примамка. Два национални вота поставиха държавните сайтове под наблюдение. Правителството разкри дългогодишен неоторизиран достъп до мрежите, през които държавните органи обменят документи. Ново министерство вече ръководи електронното управление и киберсигурността. Планирайте едновременно срещу измами със самоличност и шпионаж: защитете пощата и обмена на документи и предупреждавайте клиентите при всяка вълна от измами и преди големи промени.

2.1 Свързано население със силен мобилен навик

През октомври 2026 г. България има 6,66 милиона жители и 5,98 милиона интернет потребители, или проникване от 89,8%. Мобилните връзки са 9,26 милиона (139% от населението), а потребителските идентичности в социалните мрежи са 4,80 милиона [S14].

Криминалните данни, с които разполагаме за България, са почти изцяло трафик в Telegram, като в тях преобладават английският и руският език (глава 4). България обикновено фигурира като една държава в ценова листа за много страни, редом с Румъния, Гърция и останалата част от Европейския съюз. Публикациите на български език са малцинство, а броят им спада от юни; редът не е сравним преди и след средата на 2026 г. (§4.2).

2.2 Преминаването към еврото като примамка за измами

България прие еврото на 1 януари 2026 г. при фиксиран курс от 1,95583 лева за евро [S15][S16]. Преди прехода Министерството на вътрешните работи (МВР) предупреди гражданите за обаждания и имейли, които уж идват от банки, пощи или полицията. Такива съобщения искат данни за карти или ПИН кодове, съобщи националната обществена медия [S17]. През януари звеното за киберпрестъпност на министерството съобщи за ръст на измамите с фалшиви купувачи срещу продавачи в сайтове за обяви, с фишинг връзки, които искат данни за карти и кодове за 3-D Secure [S40].

Преходът е важен за защитниците, защото всяка нова цена, известие по сметка и формуляр за плащане дава на фишинг съобщението правдоподобен повод. Глава 8 показва, че случаите на измами, за които властите съобщиха през 2026 г., следват този модел.

2.3 Изборите и защитата на държавните системи

В България се проведоха парламентарни избори на 19 април 2026 г. и президентски избори (първи тур на 25 октомври, балотаж на 1 ноември 2026 г.). Официалните изявления за киберактивността около двата избора бяха кратки. Следобед на 19 април Министерството на електронното управление заяви, че не наблюдава повишена киберактивност срещу стратегически обекти и няма атаки за отказ на услуга [S18]. По-късно същия ден News.bg, позовавайки се на национална телевизия, съобщи, че сайтовете на министерството и на

Министерския съвет са недостъпни след кибератака. Министерството заяви, че системите му работят нормално, а сайтовете бяха достъпни отново малко след 19:00 ч. [S19].

По-късно служебен заместник-министър заяви, че в последните часове на изборния ден са наблюдавани само ограничени кибератаки [S20]. Преди октомврийския вот Държавна агенция „Национална сигурност" (ДАНС) издаде допълнителни указания за киберсигурност до всички стратегически обекти и създаде работна група за защита на изборите [S21]. Не открихме официален доклад за киберинцидент на 25 октомври; балотажът на 1 ноември не е проверен отделно, а сайтът на ЦИК не можа да бъде прочетен (**Приложение А.8**). Този доклад не заема позиция по нито един от изборите.

2.4 Дългогодишен неоторизиран достъп до държавни мрежи

На 5 август 2026 г. Министерството на иновациите и дигиталната трансформация съобщи за неоторизиран достъп до определени административни мрежи, който може да е продължил години. То е открило достъпа при внедряването на нова национална система за киберсигурност [S22]. На 18 ноември министерството заяви, че държавата е прекъснала операция, която то нарече най-продължителната и най-мащабната известна кибершпионска операция срещу българската администрация [S23].

Според министерството нападателите са имали неоторизиран достъп от 2021 г. до инфраструктурата, през която държавните институции обменят информация. Те са се придвижвали между компонентите ѝ и са събирали чувствителна информация. Проверките досега не са установили изтичане на лични данни на граждани [S23]. На брифинг министърът заяви, че са изтеглени най-малко 130 GB, или над 62 милиона страници. Според него се смята, че са замесени няколко международни хакерски групи, и няма категорични доказателства, които да ги свързват с конкретна държава [S24][S25]. Глава 7 описва какво е установено и какво не е.

2.5 Ново министерство и нов закон за киберсигурността

През май 2026 г. Народното събрание сля Министерството на електронното управление с бившето Министерство на иновациите и растежа, като създаде Министерството на иновациите и дигиталната трансформация [S26]. CERT България остава националният екип за реагиране при инциденти с компютърната сигурност [S27]. През февруари Народното събрание прие изменения в Закона за киберсигурност, които транспонират Директивата NIS2 на ЕС [S28]. На 1 октомври министерството съобщи, че Европейската комисия е прекратила наказателната процедура срещу България [S29]. Глава 10 описва какво се промени за организациите.

Официалните данни показват устойчив натиск, макар да използват различни единици и периоди. Мениджърът по киберсигурност на държавната ИТ компания „Информационно обслужване" заяви, че през 2025 г. в България са регистрирани 1 513 киберинцидента. Основно това са отказ на услуга, фишинг, имейли с представяне за друго лице и заразявания с инфостийлъри [S30]. ДАНС регистрира около 450 инцидента в стратегически обекти през 2025 г. и определи интензитета на хакерските атаки като трайно нарастващ [S31]. Двата брояча обхващат различни съвкупности и не бива да се сравняват.

ОСНОВНИ ИЗВОДИ

01

Преминаването към еврото даде на измамниците нова примамка, а в един изборен ден два държавни сайта според съобщенията бяха недостъпни по причина, която остава неизяснена.

02

Правителството съобщава за петгодишен неоторизиран достъп до държавните мрежи за обмен на документи, който министерството заявява, че е открило при внедряването на национална система за наблюдение.

03

Новото министерство и измененията по NIS2 пренареждат кой надзирава киберсигурността и колко бързо трябва да се докладват инцидентите.

ГЛАВА 3

Национална експозиция: 250 водещи организации

ТАЗИ ГЛАВА ОТГОВАРЯ НА ВЪПРОСА

Колко изложени са 250-те водещи публични и частни организации в страната, когато се оценят така, както Brandefense Atlas оценява клиент, и кой сигнал трябва да се приоритизира първи?

96 от 250

организации имаха идентификационни данни, обявени за продажба в деня на проверката

В ТАЗИ ГЛАВА

3.1 Карта на обхвата
3.2 Националната оценка на Atlas и текущите обяви по сектори
3.3 Устройства и идентификационни данни
3.4 Актуални обяви за идентификационни данни: първото, което да се приоритизира
3.5 Домейни двойници, изложени документи и споменавания
3.6 Хигиена на пощата и уеб

НАКРАТКО

Оценихме 250 водещи български организации чрез оценките за експозиция на Brandefense Atlas. Почти девет от десет имат заразени устройства, свързани с домейните им, почти всички имат исторически записи за идентификационни данни, а 96 имаха обявени за продажба идентификационни данни към момента на проверката. Два потребителски доставчика на уебпоща държат 99% от записите за идентификационни данни, затова даваме общите суми с тях и без тях. Три от пет налагат DMARC. Първо приоритизирайте актуалните обяви, след това устройствата на служителите.

3.1 Карта на обхвата

Елемент	Определение
Съвкупност	250 организации: 117 държавни или публични, 133 частни
По сектори	62 държавни органа, 31 банки и финанси, 23 търговия и холдингови групи, 23 образование, 22 енергетика и комунални услуги, 18 транспорт и логистика, 18 медии и развлечения, 16 производство и индустрия, 11 застраховане, 11 хотелиерство и туризъм, 9 телекомуникации и интернет услуги, 6 здравеопазване
Подбор	Целенасочен: държавни органи и национални портали, банки и платежни институции, държавни предприятия, пазарни лидери. Избрани по размер или системна роля, а не подредени по приходи; не е използвана публикувана българска класация на топ 250
Единица	Един проверен основен домейн на организация. Всичките 250 се разрешават в DNS (21 ноември 2026 г.)
Измервания	Заразени устройства и устройства на служители, записи от бази данни от пробиви, стийлър логове и комболистове, споменавания в тъмни чатове и в тъмната мрежа, домейни двойници, изложени документи и актуални обяви на пазари за идентификационни данни
Публични проверки	DNS, TLS и HTTP заглавки
Дата	Бройките са отчетени на 21 ноември 2026 г. Бройките на устройства, идентификационни данни и обяви включват всички записи, налични на тази дата, независимо от датата на прихващане (кумулативно, не само за 2026 г.)
Периоди	Бройките на споменавания обхващат 19 ноември 2025 г.–18 ноември 2026 г.; бройките на домейни двойници обхващат последните 30 дни

Елемент	Определение
Не са уникални лица	Едно лице може да се появи в няколко източника; едно устройство може да съдържа данни за вход в няколко организации
Непредставително	Резултатите описват този списък. Те не са национални нива на разпространение

3.2 Националната оценка на Atlas и текущите обяви по сектори

Atlas оценява всяка организация от 0 (не е наблюдаван риск) до 100; по-високите стойности означават по-голяма експозиция. Този доклад публикува само националната обобщаваща оценка за 250-те организации: 50 от 100. По сектори той показва колко организации имат всеки сигнал.

Как да четем оценките на Atlas.

Термин	Значение
Национална обобщаваща оценка	Една стойност на Atlas за всичките 250 организации: 50 от 100
Актуална обява	Идентификационни данни, свързани с домейна, предлагани за продажба към момента на проверката

Устройствата и идентификационните данни са често срещани във всеки сектор; актуалните обяви са първото, което да се приоритизира

Делът на организациите във всеки сектор със сигнала. Текущите обяви за продажба на идентификационни данни са в коралов цвят.

	Заразени устройства	Устройства на служители	Записи за идент. данни	Актуална обява	История на обявите	Домейни двойници (30 дни)	Изложени документи
Медии и развлечения (18)	94%	78%	100%	89%	89%	94%	83%
Телекомуникации и интернет услуги (9)	100%	67%	100%	78%	78%	67%	67%
Търговия и холдинги (23)	100%	70%	100%	65%	65%	87%	48%
Хотелиерство и туризъм (11)	73%	55%	100%	55%	55%	64%	45%
Образование (23)	100%	100%	100%	48%	48%	83%	39%
Банки и финанси (31)	90%	55%	97%	39%	39%	94%	23%
Застраховане (11)	82%	55%	100%	36%	36%	82%	9%
Транспорт и логистика (18)	78%	56%	100%	33%	33%	78%	11%
Държавна администрация (62)	82%	60%	94%	23%	21%	85%	26%
Енергетика и комунални услуги (22)	95%	59%	100%	18%	18%	64%	14%
Здравеопазване (6)	83%	33%	83%	17%	17%	50%	0%
Производство и индустрия (16)	62%	62%	81%	0%	0%	56%	19%

Източник: връзки на Brandefense Blackhole и методът на Atlas за 250 организации, прочетени на 21 ноември 2026 г. [S3][S4]. Записите са кумулативни, не само за 2026 г.

Сектор	Организации	Организации с актуална обява за идентификационни данни
Медии и развлечения	18	16

Сектор	Организации	Организации с актуална обява за идентификационни данни
Търговия и холдинги	23	15
Държавна администрация	62	14
Банки и финанси	31	12
Образование	23	11
Телекомуникации и интернет услуги	9	7
Хотелиерство и туризъм	11	6
Транспорт и логистика	18	6
Енергетика и комунални услуги	22	4
Застраховане	11	4
Здравеопазване	6	1
Производство и индустрия	16	0
Всички 250	250	96

Как да четем таблицата. Актуалната обява е първото, което да се приоритизира (§3.4), а след нея идват заразените устройства и записите за идентификационни данни. Публикуваме оценката на Atlas само като национална стойност.

3.3 Устройства и идентификационни данни

Търговските платформи и телекомите носят най-много асоциации със заразени устройства, почти всички извън класификацията за служители



Източник: връзки на Brandefense Blackhole и методът на Atlas за 250 организации, прочетени на 21 ноември 2026 г. [S3][S4]. Записите са кумулативни, не само за 2026 г.

Две организации от списъка предоставят потребителски услуги за уебпоща. Техните домейни са имейл адресите на стотици хиляди частни потребители. Затова почти всеки запис за идентификационни данни и всяко устройство, класифицирано като на служител, за тези домейни принадлежи на потребител, а не на персонала. Заедно те държат 76,2 милиона от 76,7 милиона записа за идентификационни данни (99,3%). Таблицата показва секторните суми без тях там, където това е от значение.

Сектор	Организации със заразени устройства	Устройства (на служители)	Записи за идентиф
Търговия и холдинги	23 от 23	87 738 (106)	
Телекомуникации и интернет услуги	9 от 9	54 366 (435 без доставчика на уебпоща)	
Банки и финанси	28 от 31	34 891 (126)	
Образование	23 от 23	32 651 (3 592)	
Държавна администрация	51 от 62	28 877 (4 057)	
Хотелиерство и туризъм	8 от 11	21 275 (61)	
Транспорт и логистика	14 от 18	16 348 (212)	
Енергетика и комунални услуги	21 от 22	11 120 (81)	
Медии и развлечения	17 от 18	10 928 (109 без доставчика на уебпоща)	
Застраховане	9 от 11	2 228 (30)	
Здравеопазване	5 от 6	575 (2)	
Производство и индустрия	10 от 16	73 (49)	
Всички	**218 от 250**	**301 070 (на служители: 8 860, без двата доставчика на уебпоща)**	

Бройките на устройствата са долни граници. Без двата доставчика на уебпоща записите за идентификационни данни се разделят на 69 075 записа от бази данни от пробиви, 220 616 реда от стийлър логове и 276 244 записа от комболистове. Заразените устройства съдържат общо около 2,96 милиона прихванати идентификационни данни за всички услуги, не само за собствените услуги на организацията.

Какво означава това.

- **Потребителските платформи носят натоварването с устройства, почти изцяло извън класификацията за служители.** Платформите за търговия и обяви, телекомите и банките имат най-много асоциации с устройства. Техните стийлър логове включват вход в сайта на организацията, така че най-вероятно това са собствените компютри на клиентите, макар собствеността да не е установена. Тези асоциации са сигнал за измами и отвличане на акаунти и сами по себе си не установяват проникване.
- **Държавната администрация и университетите носят проблема с устройствата на служителите.** Държавните органи имат 4 057 устройства, класифицирани като на служители, а образованието 3 592. Някои държавни домейни издават акаунти на граждани или на ученици и учители, така че „служител" може да включва потребители извън персонала. Рискът е повторно използване на идентификационни данни в системи, до които имат достъп същите хора.
- **Концентрацията варира.** В държавната администрация две организации държат 93% от записите за идентификационни данни в сектора; в енергетиката двете най-големи държат 26%. Секторната сума е лош ориентир за типичната организация.
- **Медианната организация е умерено засегната.** Медианната организация има 70 заразени устройства и 391 записа за идентификационни данни. Най-засегнатите отделни организации носят десетки хиляди устройства или стотици хиляди записи за идентификационни данни.

3.4 Актуални обяви за идентификационни данни: първото, което да се приоритизира

96 от 250 организации имаха поне един набор от идентификационни данни, свързан с домейна им, обявен на наблюдаван пазар за идентификационни данни към момента на проверката.

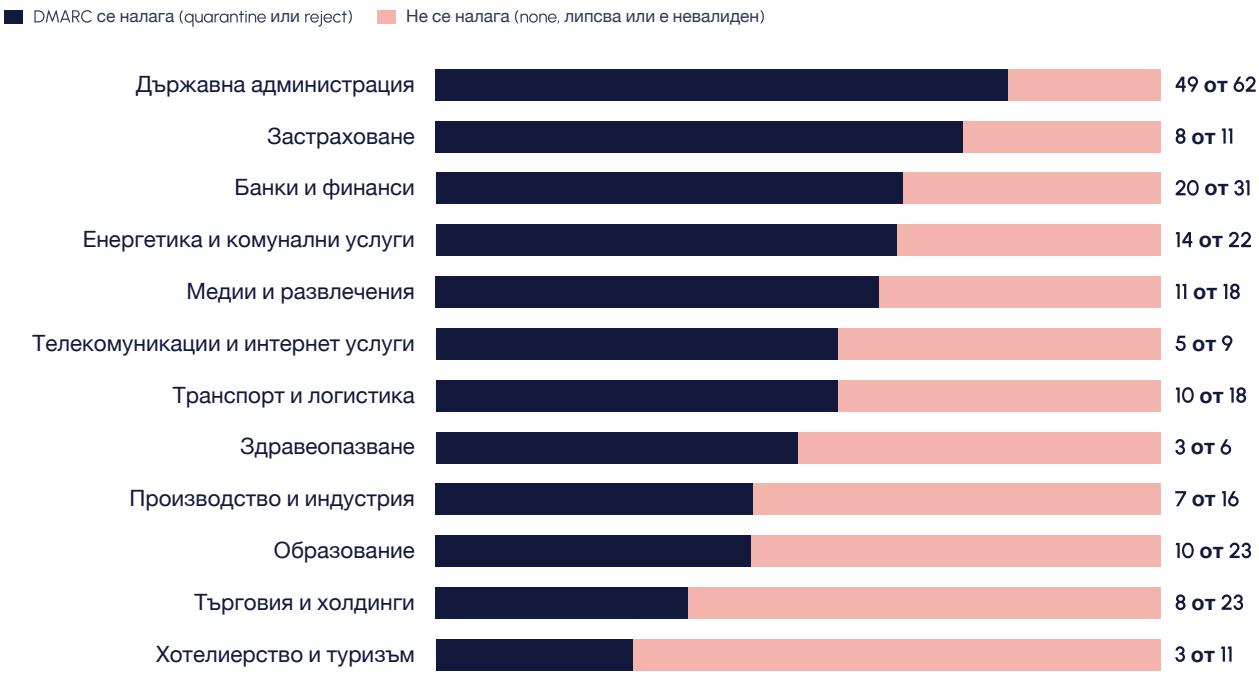
За защитника актуалната обява е най-прекият пазарен сигнал, че се предлага вход, свързан с домейна. Дали този вход все още работи, е точно това, което проверката трябва да установи. Обявата не казва колко акаунта, чии акаунти, нито дали акаунтът е активен, защитен с многофакторно удостоверяване или вече с нулирана парола. Решението, което тя подкрепя, е „проверете акаунта сега", а не „обявете пробив".

3.5 Домейни двойници, изложени документи и споменавания

- **Домейни двойници:** 200 организации имаха поне един новонаблюдаван домейн двойник през последните 30 дни. Обхватът на домейните двойници е непълен за някои организации, а домейните двойници са кандидати, а не потвърдени фишинг сайтове.
- **Изложени документи:** 78 организации имат поне един изложен документ, който споменава домейна им (общо 761).
- **Споменавания:** 55 организации са споменати в източници от тъмни чатове през последните 365 дни и 35 в източници от тъмната мрежа (onion). Най-големите бройки са при доставчиците на потребителска уебпоща, защото домейните им се появяват в списъци с идентификационни данни. Бройките на споменаванията измерват видимост, а не враждебност.

3.6 Хигиена на пощата и уеб

Държавната администрация и банките в повечето случаи налагат DMARC; търговията, хотелиерството и образованието в повечето случаи не



Източник: публични проверки на DNS, TLS и началната страница на 250 домейна от Brandefense, 21 ноември 2026 г. [S5].

Резултати от нашите публични проверки на DNS, TLS и началните страници [S5]:

Контрол	Резултат (от 250, освен ако не е посочено)	Прочит
DMARC reject	69	Подправената поща от домейна би трябвало да бъде отхвърлена
DMARC quarantine	79	Подправената поща би трябвало да отиде в спам
DMARC p=none или липсва	102 (60 none, 42 липсва)	Няма налагане; подправянето на домейна е по-лесно
SPF, завършващ с -all / ~all / ?all / друго / няма	160 / 73 / 2 / 5 / 10	10 домейна не публикуват SPF политика
Открит DKIM	163	Липсата не доказва липса на DKIM
Наблюдаван DS запис (DNSSEC делегиране)	51	Не е наблюдаван DS запис за 199 домейна; DS записът сам по себе си не доказва валидна верига на доверие
Невалиден TLS сертификат	11 от 238 проверени	Изтекли, несъответстващи или недоверени сертификати
HSTS на началната страница	110 от 197 достъпни	Много сайтове не налагат HTTPS за завръщащи се посетители
Доставчик на поща	57 Microsoft 365, 28 Google, 8 без MX	Останалите използват собствена или регионална поща

Уеб проверките не можаха да бъдат завършени за 53 сайта. Техните DNS проверки са пълни.

Държавната администрация води при DMARC и DNSSEC; търговията и хотелиерството изостават. От 62 държавни органа 49 налагат DMARC, а държавните домейни са 29 от 51-те с DS запис. В банките и финансите 20 от 31 организации налагат DMARC. Най-малко налагат търговията (8 от 23), хотелиерството (3 от 11) и образованието (10 от 23). По пасивния хигиенен индекс (приложение A.5; 0–100, по-високо означава по-слабо) най-слаби стойности на индекса по сектори имат хотелиерството (50), транспортът (48), образованието и производството (по 47). Най-силни са държавната администрация (35) и медиите (36).

ОСНОВНИ ИЗВОДИ

01

Асоциациите с устройства и идентификационни данни са широко разпространени в списъка; те изискват проверка, а не тревога.

02

Актуалната обява за идентификационни данни е най-прекият пазарен сигнал, затова е първото, което да се приоритизира.

03

Два от пет домейна не налагат DMARC и само 51 от 250 публикуват DNSSEC делегиране.

ГЛАВА 4

Какво виждаме в тъмната мрежа

ТАЗИ ГЛАВА ОТГОВАРЯ НА ВЪПРОСА

Какво публикуват престъпниците конкретно за България и кои оферти са важни за защитниците?

1 757

уникални публикации в маркирания набор, които се отнасят конкретно до България

В ТАЗИ ГЛАВА

4.1 Карта на обхвата | 4.2 Платформи, езици и обем | 4.3 Престъпни категории след преглед | 4.4 Данни на застрахователни клиенти: най-значимите твърдения за данни през годината | 4.5 Твърдения с правителствена тематика | 4.6 Казуси | 4.7 Какво добавят форумите

НАКРАТКО

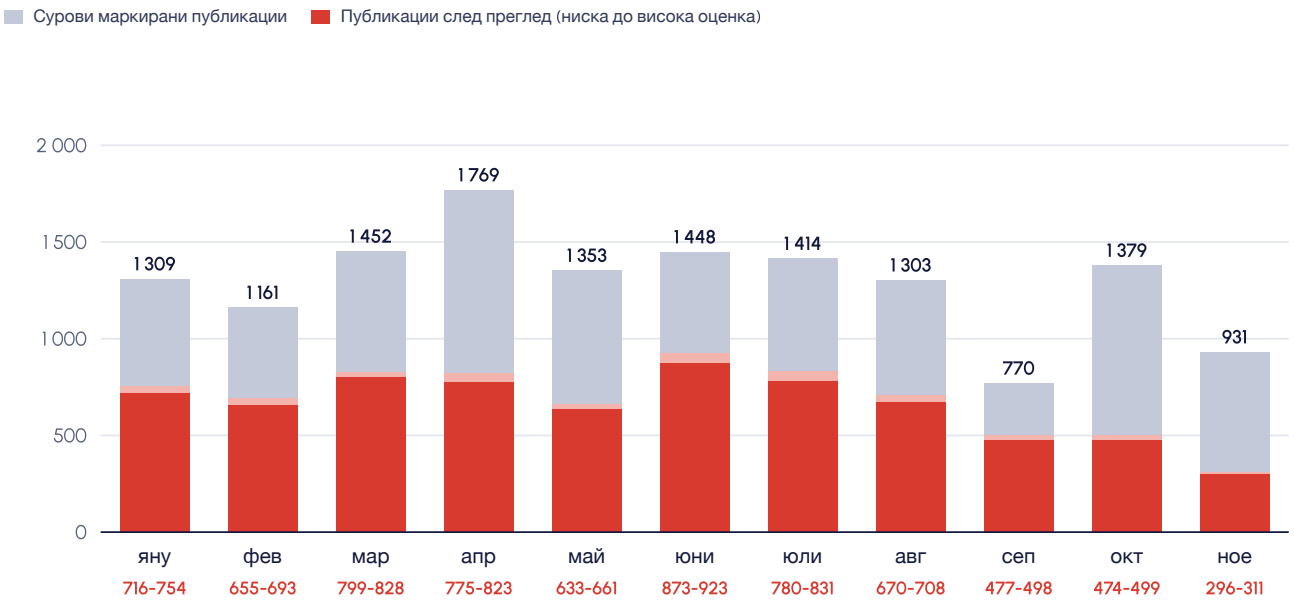
Повечето подземен трафик с маркер „България" е реклама в Telegram на английски и руски, в която България е една от много държави. По-малък набор засяга конкретно България: банкови и платежни сметки, документи за самоличност, резултати от проверка на карти, повтарящи се комболистове „Bulgaria" и списъци с данни за уебпоща. Най-сериозните оферти през 2026 г. твърдят, че предлагат данни на застрахователни клиенти и правителствен достъп. Четете бройките за България, а не общия обем, и проверявайте произхода на всяко твърдение преди коментар.

4.1 Карта на обхвата

Елемент	Определение
Източник	Brandefense Blackhole: канали и групи в Telegram, набор от киберпрестъпни форуми, сайтове за пейстове и Discord
Определение за държава	Публикации, маркирани като отнасящи се до България, насочени към нея или споменаващи я
Период	Време на публикуване 1 януари–18 ноември 2026 г. (ноември частично)
Маркиран набор	14 289 преброени публикации; 14 286 уникални
Обединен корпус	24 148 уникални публикации: маркираният набор плюс 9 862 свързани публикации
Маркиран набор след преглед	7 148–7 529 публикации
Набор, специфичен за България	1 757 уникални маркирани публикации (3 325 в обединения корпус), в които България е темата, а не един ред в списък с много държави
Не е установено	Че маркирана публикация е насочена към България, че дадено твърдение е вярно или че две публикации се отнасят до един и същ файл

4.2 Платформи, езици и обем

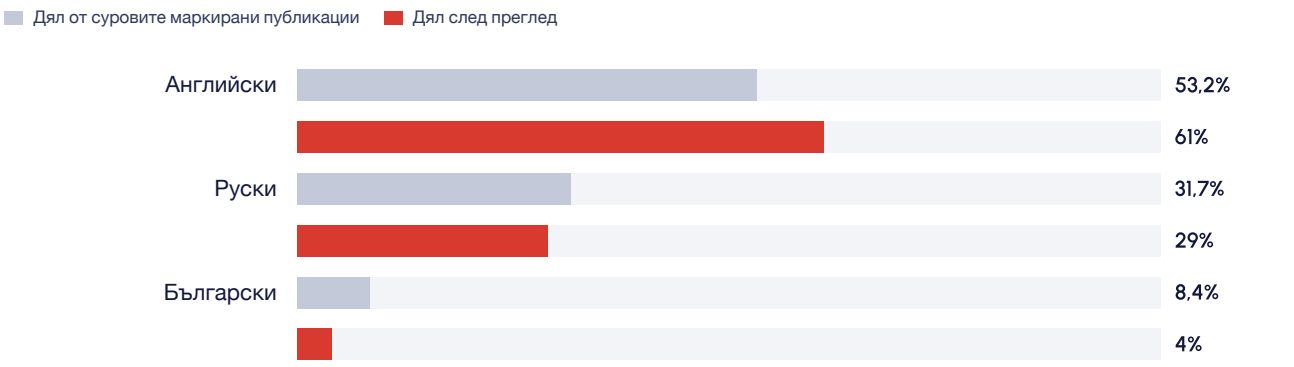
Маркираният за България обем остава между 770 и 1 769 публикации месечно, без пиковете от шаблони при Румъния и Гърция



Източник: Brandefense Blackhole, публикации, маркирани като отнасящи се до България, дати на публикациите 1 януари-18 ноември 2026 г., ноември частично [S1]. Бройките след преглед са горна граница.

Показател	Стойност
Дял на Telegram в маркираните публикации	98,6% (14 085)
Публикации във форуми	165 (плюс 305 свързани публикации във форуми)
Пейст, Discord, onion сайтове	27, 12, 0
Английски / руски / български / турски	53,2% / 31,7% / 8,4% / 1,7% от суровите публикации
След преглед: английски / руски / български	61% / 29% / 4%
Сурови публикации на месец	770–1 769 в пълните месеци; 931 в частичния ноемврийски период

Маркерът за България идва главно от английски и руски; публикациите на български са малък дял



Telegram носи 98,6% от маркираните публикации. Езиковите етикети може да се припокриват. Източник: Brandefense Blackhole, публикации, маркирани като отнасящи се до България, дати на публикациите 1 януари-18 ноември 2026 г., ноември частично [S1]. Бройките след преглед са горна граница.

България не показва пикове от шаблони. Румъния и Гърция имат над 300 000 маркирани публикации и през януари, и през февруари, заради масова реклама за много държави. Маркерът за България обхваща 1 161–1 309 публикации в тези месеци. След преглед остават 474–923 публикации във всеки пълен месец (януари–октомври); частичният ноемврийски период съдържа 296–311.

Редът се прекъсва в средата на годината. Публикациите, маркирани като български език, спадат от 283 през май до 38 през юни и след това остават под 10 на месец. Месечните редове не са сравними преди и след средата на 2026 г., затова не тълкуваме промените от юни нататък като тенденции в заплахите.

4.3 Престъпни категории след преглед

Документите за самоличност, търговията със сметки и картовите данни водят сред публикациите, специфични за България



Източник: Brandefense Blackhole, публикации, маркирани като отнасящи се до България, дати на публикациите 1 януари–18 ноември 2026 г., ноември частично [S1]. Бройките след преглед са горна граница.

Категория	Публикации след преглед (мин.–макс.)	Публикации, специфични за България	Какво съдържа
Изтичания на данни и бази данни	2 842–2 890	85	Главно два шаблона за много държави: обновявания на наличността в магазини за карти и бази с контакти за „физически лица"; офертите, специфични за България, са много по-малко
Търговия с банкови и платежни сметки	2 040–2 151	291	Купуване, наемане и продажба на български банкови, финтех и платежни сметки с български IBAN
Кардинг	1 771–1 808	257	Резултати от проверка на карти, обновявания на магазини за карти, които включват България, купувачи на български карти
KYC (познаване на клиента) и документи за самоличност	1 567–1 672	341	Потвърдени акаунти, комплекти от лични карти и селфита, шаблони на документи

Категория	Публикации след преглед (мин.-макс.)	Публикации, специфични за България	Какво съдържа
Фишинг и измами	330–349	19	Софтуер за изпращане на SMS, страници за измами, „трафик" за измами
Комболистове	208–228	119	Списъци с идентификационни данни с етикет „Bulgaria" и списъци с данни за уебпоща
Зловреден софтуер и експлойти	188–197	19	Продажба на инструменти и обсъждане на експлойти, предимно глобални
Продажба на достъп	152–181	12	Административни панели, администраторски акаунти за сайтове, отдалечени сървъри
Стийлър логове	133–147	57	Продажба на логове, списъци с акаунти „cracked and inboxed" (с разбита парола и проверен достъп до пощата)
Рансъмуер (препредавания)	21	21	Препредавания на твърдения от сайтове за изтичане (глава 7)
DDoS и хактивизъм	11	3	Малко; вж. глава 6

Категориите се припокриват и не бива да се събират. Редът за рансъмуер брои препредавания в маркирания набор и не е част от графика c02. Прегледаните категории за изтичания на данни и кардинг са надути от два повтарящи се шаблона за много държави. Един магазин за карти публикува 1 073 обновявания на наличността, в които България е сред десетки държави, а реклама за база с контакти е препубликувана над 1 200 пъти. Колоната за България е по-добрият ориентир за това, което засяга българските организации.

Посочени цени. В прегледаните публикации с посочена цена медианата на поисканата цена е 110 USD за банкова или платежна сметка и 100 USD за KYC и услуги с документи. Офертите за достъп имат медиана 400 USD (малко стойности), а комболистовете 50 USD. Посочените единични български оферти варират от 10 USD за твърдян правителствен пощенски панел до 250 USD за готова сметка в българска банка (глава 8); медианите по-горе включват публикации за много държави. Това са поискани цени, а не завършени продажби.

4.4 Данни на застрахователни клиенти: най-значимите твърдения за данни през годината

Между края на август и средата на септември 2026 г. няколко площадки рекламираха клиентски данни, приписвани на български застрахователи. Нито една оферта не е независимо потвърдена и не сме получили нито един файл.

Дата	Твърдян набор от данни	Твърдени полета	Твърдян обем	Площадка	Публикация
30 август	„Bulgarian insurance company customer database", описана като извлечена от записи с национални идентификационни номера	Клиентски ID, вид документ, име, пол, дата на раждане, адрес, телефон, имейл	„2.2M+" записа, година 2025	Telegram канал за търговия с контакти	B01
10 и 16 септември	„Bulgaria insurance database" с примерен заглавен ред	ID на лице, вид документ (ЕГН), имена на кирилица и латиница, пол, дата на раждане, област, град, адрес, телефон, имейл	Не е посочен	Киберпрестъпен форум, продажба през Telegram	B02

Дата	Твърдян набор от данни	Твърдени полета	Твърдян обем	Площадка	Публикация
1 **септември (съобщено на** 10 **септември)**	Записи, приписвани на голям застраховател, съобщени от медии, препредаващи публикация във форум; продавачът посочва слабо защитен API на клиентския портал	Национални идентификационни номера и номера на паспорти, адреси, контакти	3 134 269 реда	Форум (медийна публикация)	Няма [S32]
Септември (съобщено на 26 **септември)**	Записи, свързани с втори застраховател, съобщени от разследваща медия и препредадени от сайт за новини в сигурността	Имена, ЕГН, адреси, телефонни номера	„Над 300 000“	Не е посочена	Няма [S34]

Какво е потвърдено официално. На 24 септември Комисията за защита на личните данни (КЗЛД) отговори на заявление за достъп до обществена информация. Тя потвърди уведомления за нарушение на сигурността на личните данни от две застрахователни компании от една група на 3 август и от втори застраховател на 11 септември. КЗЛД заяви, че е образувала производства [S34]. Тя не потвърди броя на записите. Според същата публикация един от застрахователите отрича проникване в собствените си информационни системи [S34].

Какво означава това за защитниците. Публикациите не показват от коя система идват данните, а полетата съвпадат с това, което съхраняват много организации. Какъвто и да е произходът, рекламираните полета включват единния граждански номер (ЕГН), дата на раждане, адрес и телефон. Банките, телекомите и застрахователите, които проверяват обаждащите се с тези полета, трябва да приемат, че те са известни на престъпниците.

КАРТА НА ПУБЛИКАЦИЯ B01 30 авг 2026

Lead-trading channel Telegram канал за търговия с лийдове · Telegram · английски

ОРИГИНАЛ

```
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]
```

ПРЕВОД

База данни с клиенти на българска застрахователна компания: над 2,2 млн. записа 🇧🇬
Структурирана база данни с приблизително над 2,2 млн. клиентски записа, свързани с българска застрахователна компания.
Източник: база данни с клиенти на български застраховател (извлечена от ЕГН/[държавен регистър]).
Година: 2025
Полета: клиентски номер, вид документ, вид клиент, име, пол, дата на раждане, държава, област, град, адрес, пощенски код, телефон и имейл.
Лично съобщение в Telegram: [контактът е премахнат]

Бележка. ЕГН е българският личен идентификационен номер. Описанието на източника е собствено твърдение на публикуващия.

КАКВО МОЖЕМ ДА УСТАНОВИМ	Предложението, заявените полета, заявената година и заявеният обем.
КАКВО НЕ Е УСТАНОВЕНО	Кой застраховател, дали данните изобщо идват от застраховател, каквато и да е връзка с държавни регистри, каквато и да е продажба.

КАРТА НА ПУБЛИКАЦИЯ B02 10 сеп 2026

lauraallen Форум за киберпрестъпност · Форум · английски, заглавен ред на извадката на латиница, редове от извадката на български

ОРИГИНАЛ

```
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]
```

ПРЕВОД

База данни на застраховател в България
За поръчка: лично съобщение в Telegram: [контактът е премахнат]
Код: 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
[редовете от извадката с имена, лични номера и адреси са премахнати]

Бележка. Редовете от извадката съдържат вид документ "EGN". Същата публикация беше повторена на 16 септември.

КАКВО МОЖЕМ ДА УСТАНОВИМ	Предложението, структурата на полетата и това, че са публикувани редове от извадка.
КАКВО НЕ Е УСТАНОВЕНО	Кой застраховател, дали извадката е истинска, размерът на файла, каквато и да е продажба.

4.5 Твърдения с правителствена тематика

Дата	Наблюдавана публикация	Нашият прочит	Публикация
5 април	Продавач във форум предлага „Bulgarian eGov mail admin panel" за 10 USD, като твърди, че панелът може да създава неограничен брой правителствени пощенски акаунти в пет домейна, заедно с панели за други държави	Непотвърдено твърдение за достъп; ниската цена и списъкът с много държави подсказват препродавач на откраднати данни за вход в пощенски акаунти, а не доказват пробив в панел	B04
10-11 август	Тема във форум със заглавие „[BG] Bulgaria Starred Bears" твърди, че разкрива данни от български системи, със снимки на екрана, описани като разузнаване, първоначален достъп, придвижване в Linux и работа с бази данни; препредадена от канал за хакерски новини	Непотвърдено; препредадено пет-шест дни след първото разкритие на правителството за дългогодишен неоторизиран достъп (§2.4); няма общ елемент, който да свързва двете	B03
11 август	Автоматичен качващ акаунт във форум публикува малък файл с редове имейл и парола за пощенския домейн на министерство	Съвместимо с редове от стийлър логове или повторно използвани пароли от собствените устройства на потребителите (извод); няма доказателства за пробив в пощенски сървър	Няма

Дата	Наблюдавана публикация	Нашият прочит	Публикация
22 август	Група, която се нарича Enigma Group, публикува според нея бекенд VPN и мрежови адреси на държавна система в транспортния сектор, взети от инструмент за проверка на достъпността на администратор	Непотвърдено; ако е истинско, това са данни от разузнаване, а не доказателство за достъп	B12

Какво означава това за защитниците. През 2026 г. публикациите с правителствена тематика са за пощенски кутии и достъп, а не за бази данни на населението. Евтин „панел" или файл с няколко реда за домейн на министерство обикновено означава откраднати потребителски данни за вход. Това все пак е важно. През юли CERT България съобщи за имейли с бомбени заплахи до държавни институции, изпратени от отвлечени акаунти, които преминават проверките SPF, DKIM и DMARC [S35]. Удостоверяването на пощата не може да спре съобщение, изпратено от истинска пощенска кутия, която някой друг контролира.

КАРТА НА ПУБЛИКАЦИЯ B04 — 5 апр 2026

DuperKinger123 Форум за киберпрестъпност · Форум · английски

ОРИГИНАЛ

```
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]
```

ПРЕВОД

Административен панел за българска държавна поща (eGov) - 10$ (може да създава неограничен брой държавни пощенски акаунти в 5 различни домейна)
[предложенията за панели и пощенски кутии на държавни пощи в други държави са пропуснати]
Ако искате да купите нещо от това или имате въпроси, пишете ми в Telegram [контактът е премахнат]

КАКВО МОЖЕМ ДА УСТАНОВИМ	Предложението и цената.
КАКВО НЕ Е УСТАНОВЕНО	Коя платформа, дали панелът съществува, създаден ли е акаунт, каквато и да е продажба.

КАРТА НА ПУБЛИКАЦИЯ B03 — 11 авг 2026

Relay channel

Telegram канал за хакерски новини, препредаващ тема от форум · Telegram · английски

ОРИГИНАЛ

```
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.
```

ПРЕВОД

БЪЛГАРИЯ: Извършител на заплахи публикува предполагаеми данни, свързани с държавата
Извършител на заплахи е публикувал материал със заглавие "[BG] Bulgaria Starred Bears", като твърди, че разкрива данни, свързани с български системи.
* Публикацията съдържа множество предполагаеми доказателства за компрометиране.
* Показаните файлове включват препратки към разузнаване, първоначален достъп, придвижване в Linux среда, кръстосано съпоставяне на бази данни и SSRF/прокси обработчик.
* [...] конкретните твърдения остават непроверени.

Бележка. Самата тема не е преглеждана за този доклад.

КАКВО МОЖЕМ ДА УСТАНОВИМ	Че тема с това заглавие е публикувана и препредадена и как препредаването я описва.
КАКВО НЕ Е УСТАНОВЕНО	Каквото и да е проникване, каквито и да е данни, извършителят, каквато и да е връзка с проникването, разкрито от правителството на 5 август.

КАРТА НА ПУБЛИКАЦИЯ B12 — 22 авг 2026

Enigma Group Форум за изтичания · Форум · английски

ОРИГИНАЛ

```
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.
```

ПРЕВОД

Здравейте, ние сме Enigma Group и днес решихме да публикуваме IP адресите на BACKEND системата на [държавна система в транспортния сектор]. Изтичането съдържа IP адреси на VPN сървъри, WAN [...] Цялата тази информация е взета от инструмента на администратора за проверка на работоспособността.

КАКВО МОЖЕМ ДА УСТАНОВИМ	Твърдението и посоченият източник.
КАКВО НЕ Е УСТАНОВЕНО	Дали адресите са истински или актуални; какъвто и да е достъп до системата.

4.6 Казуси

Всеки случай следва една и съща структура: твърдение, хронология, какво можем да установим, алтернативи, ограничения и пропорционална реакция.

A СЛУЧАЙ A

Няколко оферти за данни на застрахователни клиенти в рамките на три седмици

Карта на публикация B01 · 30 авг 2026 · Telegram канал за търговия с лийдове · Застраховане

НЕПОТВЪРДЕНИ ТВЪРДЕНИЯ; ПОТВЪРДЕНИ УВЕДОМЛЕНИЯ ОТ ТРИ ЗАСТРАХОВАТЕЛЯ В ДВЕ ГРУПИ

Твърдение	На 30 август канал за търговия с контакти предложи „2.2M+" записа на клиенти на български застраховател. На 10 и 16 септември продавач във форум публикува образец „Bulgaria insurance database".
Хронология	Регулаторът получи уведомления за нарушение от две компании от една застрахователна група на 3 август и от втори застраховател на 11 септември [S34]. На 10 септември медии съобщиха за оферта във форум, която назовава един застраховател и е забелязана за първи път на 1 септември [S32]. По-късно разследваща медия съобщи за над 3 милиона записа, свързани с единия застраховател, и над 300 000 за другия [S34].
Какво можем да установим	Че между 30 август и 16 септември се появиха поне три оферти за данни на клиенти на български застрахователи и че регулаторът е получил уведомления от три застрахователни дружества от две групи. Публикациите не установяват коя оферта на кое уведомление съответства, нито че файловете са еднакви.
Алтернативи	Един набор от данни, препродаван под няколко заглавия; отделни набори от двете застрахователни групи; събрани данни от други източници, преетикетирани като застрахователни.
Реакция	Застрахователите и техните брокери трябва да сравнят всеки образец със собствените си схеми за експорт и да прегледат достъпа на партньори и до API на портала. Банките и телекомите трябва да третират ЕГН, датата на раждане и адреса като публични, когато проверяват обаждащите се.
ИЗВОДЪТ	**Приемете, че ЕГН, датата на раждане и адресът са известни на престъпниците; застрахователите трябва да сравнят всеки образец със собствените си експорти преди коментар.**

B

СЛУЧАЙ B

Твърдение за „правителствени данни“ дни след официално разкритие

НЕПОТВЪРДЕНО ТВЪРДЕНИЕ

Карта на публикация B03 | 11 авг 2026 | Telegram канал за хакерски новини, препредаващ тема от форум | Държавна администрация

Твърдение	На 10-11 август препредавания съобщиха за тема във форум със заглавие „[BG] Bulgaria Starred Bears“, която твърди, че разкрива данни от български системи. Снимките на екрана според препредаването показват разузнаване, първоначален достъп, придвижване в Linux и съпоставяне на бази данни.
Хронология	Първото разкритие на министерството за дългогодишен неоторизиран достъп до административни мрежи е от 5 август [S22]. Препредаванията последваха пет-шест дни по-късно. По-пълното изявление на министерството дойде на 18 ноември [S23].
Какво можем да установим	Че участник във форум отправи твърдение с правителствена тематика и технически снимки на екрана скоро след разкритието. Самата тема не е преглеждана за този доклад. Няма общ елемент, който да свързва публикацията с неоторизирания достъп, описан от министерството.
Алтернативи	Участник, който се възползва от медийното отразяване; несвързано проникване; истински материал от разкрития неоторизиран достъп.
Реакция	Екипите по сигурността в държавната администрация трябва да сравнят снимките на екрана, ако бъдат получени, с известните индикатори на инцидента преди всякакъв публичен коментар.
ИЗВОДЪТ	**Твърдение във форум след официално разкритие не е доказателство за разкритото проникване; сравнете индикаторите преди коментар.**

C

СЛУЧАЙ C

Правителствени пощенски кутии се продават евтино

НАБЛЮДАВАНА ОФЕРТА (ЕДНА ПУБЛИКАЦИЯ)

Карта на публикация B04 | 5 апр 2026 | Форум за киберпрестъпност | Държавна администрация

Твърдение	На 5 април продавач във форум предложи „Bulgarian eGov mail admin panel“ за 10 USD, заедно с правителствени пощенски панели от други държави.
Какво можем да установим	Офертата и цената ѝ. Правителствен пощенски „панел“ на тази цена е по-съвместим с откраднати потребителски или администраторски данни за вход, отколкото с контрол над пощенска платформа. Публикацията не показва кое от двете е.
Защо е важно	Офертата се свързва с официално наблюдение: през юли CERT България съобщи за имейли със заплахи, изпратени от отвлечени акаунти, които преминават удостоверяването на пощата [S35].
Реакция	ИТ екипите на държавни и общински органи трябва да прегледат администраторските влизания в пощенските платформи, да въведат устойчиво на фишинг MFA за администраторите на пощата и да настроят сигнали при масово създаване на акаунти.
ИЗВОДЪТ	**Третирайте евтината оферта за правителствен пощенски панел като непотвърдена оферта за достъп; като мярка за планиране прегледайте влизанията на администраторите на пощата и въведете устойчиво на фишинг** MFA.

D

СЛУЧАЙ D

Месечни комболистове „Bulgaria“ и списъци с данни за уебпоща

ПОВТАРЯЩИ СЕ ОФЕРТИ

Карта на публикация B05 | 20 апр 2026 | Форум за киберпрестъпност | Всички сектори

Твърдение	Една марка на продавач публикува комболист „Database: Bulgaria, Email:Password, FRESH“ поне шест пъти между януари и октомври, от 68 000 реда през януари до 126 000 през април. Втора марка публикува подобни списъци с 56 000–150 000 реда.
Хронология	Отделни автори рекламираха списъци с „валидни“ акаунти във водеща българска уебпоща. Един предложи „1k valids … able to be logged in and view emails“ през февруари; друг публикува списък „338X … freshly cracked and inboxed“ през август. Няколко инструмента за проверка на поща, рекламирани през октомври и ноември, посочват същата услуга като поддържана.
Какво можем да установим	Постоянно предлагане на списъци с идентификационни данни с етикет „Bulgaria“ и на инструменти за тестването им. Публикациите не показват произхода, припокриването или валидността на списъците.
Алтернативи	Преопаковани стари данни от пробиви; списъци, създадени от стийлър логове; смесица от двете.
Реакция	Организациите, чиито служители използват лична уебпоща за работа, трябва да я блокират за корпоративни регистрации и да следят за адреси на служители в такива списъци. Потребителите на уебпоща се нуждаят от MFA.
ИЗВОДЪТ	**Очаквайте български списъци с идентификационни данни всеки месец; блокирайте личната уебпоща за работа и изисквайте MFA.**

КАРТА НА ПУБЛИКАЦИЯ B05 — 20 апр 2026

thejackal101 Форум за киберпрестъпност · Форум · английски

ОРИГИНАЛ

```
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]
```

ПРЕВОД

База данни: България Тип: имейл : парола Дата: [20/APR/2026] Combo: [126 K++] Състояние на редовете: ПРЕСНИ | HQ
Скрито съдържание. Трябва да отговорите в тази тема, за да видите съдържанието [...]
За още пресни логове: [връзката е премахната]

Бележка. Същата марка е публикувала списъци в този формат поне шест пъти между януари и октомври.

КАКВО МОЖЕМ ДА УСТАНОВИМ	Предложението, заявеният размер и заявената свежест.
КАКВО НЕ Е УСТАНОВЕНО	Произходът, припокриването с по-ранни списъци, валидността на който и да е ред.

КАРТА НА ПУБЛИКАЦИЯ B06 — 8 авг 2026

kookiegst Форум за киберпрестъпност · Форум · английски

ОРИГИНАЛ

```
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
```

ПРЕВОД

338 БРОЯ [уеб поща] БЪЛГАРИЯ FA HITS, ТОКУ-ЩО РАЗБИТИ И С ДОСТЪП ДО ПОЩАТА, МОЛЯ ОСТАВЕТЕ ХАРЕСВАНЕ И ПОДКРЕПА [...] ЗАБЕЛЕЖКА: НЯКОЙ ДРУГ МОЖЕ ДА ЗАЯВИ АКАУНТА ПРЕДИ ВАС

Бележка. "Hits" и "inboxed" означават, че публикуващият твърди, че паролите са тествани и пощенските кутии са отворени.

КАКВО МОЖЕМ ДА УСТАНОВИМ	Твърдението за 338 тествани пощенски кутии в българска услуга за уеб поща.
КАКВО НЕ Е УСТАНОВЕНО	Какъвто и да е пробив в услугата; валидността; чии са пощенските кутии.

КАРТА НА ПУБЛИКАЦИЯ B07 16 фев 2026

UHQCombos Форум за кракване · Форум · английски

ОРИГИНАЛ

```
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]
```

ПРЕВОД

Имам 1k валидни [уеб поща], скоро може да станат общо 2k, във всички може да се влезе и да се четат имейлите и т.н., предложете цена, пишете ми тук или в Telegram [контактът е премахнат]

КАКВО МОЖЕМ ДА УСТАНОВИМ	Предложението.
КАКВО НЕ Е УСТАНОВЕНО	Валидността, произходът, каквато и да е продажба.

E

СЛУЧАЙ E

Бази данни на клиенти на търговци и здравна платформа

НЕПОТВЪРДЕНИ ТВЪРДЕНИЯ

Карта на публикация B08 | 18 фев 2026 | Форум за пробиви | Търговия и здравеопазване

Твърдение	На 29 януари продавач във форум предложи за 50 USD 32 683 записа, за които твърди, че са от здравна платформа с български потребители, пробита два дни по-рано. На 18 февруари продавач предложи база данни на онлайн търговец с „около 4M записа", сортирана до 1,8 милиона реда. Блог за наблюдение на пробиви, препредаден в нашите данни, съобщи, че през февруари се продават клиентски записи и поръчки на търговец на мебели.
Какво можем да установим	Офертите, твърдените полета (имена, имейл, телефон, град, дата на раждане, пол или адрес) и цените. Нито една не е потвърдена и, доколкото открихме, нито една от тези организации не беше потвърдила пробив към нашата крайна дата.
Алтернативи	По-стари експорти; извлечени или събрани данни; истински пробиви.
Реакция	Компаниите за електронна търговия трябва да проверят за масови експорти и злоупотреба с API на твърдените дати и да подготвят предупреждения към клиентите за фишинг с тематика поръчки.

ИЗВОДЪТ **Проверете масовите експорти и API логовете на твърдените дати; предупредете клиентите за фишинг с тематика поръчки.**

КАРТА НА ПУБЛИКАЦИЯ B08 18 фев 2026

Jurak Форум за пробиви · Форум · английски

ОРИГИНАЛ

```
[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
```

ПРЕВОД

[онлайн търговец] е платформа за онлайн търговия в България, която предлага потребителски стоки [...] Данните съдържат около 4M записа, сортирах ги до около 1,8M уникални реда (на около 400k реда липсват имена или телефонни номера). име, адрес, имейл, телефон
Изпратете съобщение с вашето предложение

КАКВО МОЖЕМ ДА УСТАНОВИМ	Предложението, заявените полета и броеве.
КАКВО НЕ Е УСТАНОВЕНО	Произходът, възрастта, какъвто и да е пробив при търговеца, каквато и да е продажба.

КАРТА НА ПУБЛИКАЦИЯ B17 29 яну 2026

temporary Форум за пробиви · Форум · английски, редове от извадката на български

ОРИГИНАЛ

```
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]
```

ПРЕВОД

Здравейте, Breach Forums, продавам базата данни на [здравна платформа] [...] Общо редове: 32 683 Дата на пробива: 27-01-2026 Цена: 50 $ Полета: имейл, име, фамилия, град, дата на раждане, пол
Извадки: [редовете с имена, имейли, телефонни номера и дати на раждане са премахнати]

КАКВО МОЖЕМ ДА УСТАНОВИМ	Предложението, заявените полета, заявената дата на пробива и цената.
КАКВО НЕ Е УСТАНОВЕНО	Какъвто и да е пробив в платформата; че извадката е истинска; каквато и да е продажба.

F

СЛУЧАЙ F

Рекламира се достъп до инфраструктура и устройства

НЕПОТВЪРДЕНИ ТВЪРДЕНИЯ

Карта на публикация B16 | 23 авг 2026 | Форум за изтичания | Устройства и инфраструктура

Твърдение	На 23 август автор във форум предложи адреси, потребителски имена и пароли за 140 камери в България, с връзки към кадри. През февруари продавач предложи администраторски достъп до уебсайта на българска компания за събития за 50 EUR. През април потребител в чат заяви, че има достъп до портала за разработчици на българска банка, и попита дали си струва да го продаде.
Какво можем да установим	Офертите и твърденията. Нито едно не е потвърдено; твърдението за банковия портал е едно съобщение в чат без доказателства.
Защо е важно	Изложените в интернет камери и контролери са повтаряща се входна точка. През ноември CERT България предупреди за атаки в Европа срещу изложени в интернет контролери за хладилни системи [S37], а Z-Pentest заяви, че контролира контролен панел на оранжерия в България (глава 6).
Реакция	Премахнете паролите по подразбиране от камерите и контролерите и изведете интерфейсите им за управление извън интернет.
ИЗВОДЪТ	**Премахнете паролите по подразбиране и изведете управлението на камерите и контролерите извън интернет.**

КАРТА НА ПУБЛИКАЦИЯ B16 23 авг 2026

updap (forum poster) Форум за изтичания · Форум · английски

ОРИГИНАЛ

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

ПРЕВОД

140 камери в България IP:PORT,USER,PASS с връзки към снимки
Все още не сте отключили съдържанието на тази публикация. [...]

КАКВО МОЖЕМ ДА УСТАНОВИМ	Твърдението за 140 входни данни за камери.
КАКВО НЕ Е УСТАНОВЕНО	Чии са камерите, валидността, какъвто и да е достъп.

КАРТА НА ПУБЛИКАЦИЯ B09 23 фев 2026

Commando Форум за пробиви · Форум · английски

ОРИГИНАЛ

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

ПРЕВОД

Продавам администраторски достъп до уебсайта на българска [компания за събития]
Вид достъп: администраторски акаунт за уебсайт
Държава: България
Приходи: [сумата е премахната]
Цена: 50 €

КАКВО МОЖЕМ ДА УСТАНОВИМ	Предложението и цената.
КАКВО НЕ Е УСТАНОВЕНО	Дали акаунтът работи, каквато и да е продажба.

КАРТА НА ПУБЛИКАЦИЯ B13 29 апр 2026

wat4ri Telegram чат на хакерски форум · Telegram · английски

ОРИГИНАЛ

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

ПРЕВОД

имам достъп до dev портал на [българска банка], изобщо струва ли си да го продавам? lol

КАКВО МОЖЕМ ДА УСТАНОВИМ	Съобщението в чата.
КАКВО НЕ Е УСТАНОВЕНО	Какъвто и да е достъп; кой портал; каквато и да е продажба.

4.7 Какво добавят форумите

Форумите дадоха само 165 маркирани публикации, но съдържат най-конкретните твърдения: бази данни на застрахователи, търговци и здравна платформа, правителствения пощенски панел и серията комболистове. Много други попадения във форуми са глобални списъци, в които България е сред десетки държави. Купувачите също публикуваха заявки: „looking for a leak for Slovakia and Bulgaria" (юни и септември), комплекти български документи за самоличност за измами с проверка (септември и ноември) и български банкови сметки (глава 8).

ОСНОВНИ ИЗВОДИ

01

Суровият обем е предимно реклама за много държави; четете набора, специфичен за България.

02

Данните на застрахователни клиенти с ЕГН бяха най-значимото твърдение за данни през годината, а регулаторът потвърди уведомления за нарушение от три застрахователни дружества от две групи.

03

Публикациите с правителствена тематика са за пощенски кутии и достъп; третирайте евтиния „панел" като непотвърдена оферта за достъп и, като мярка за планиране, прегледайте влизанията на администраторите на пощата.

ГЛАВА 5

Примери за насочване по сектори

05

ТАЗИ ГЛАВА ОТГОВАРЯ НА ВЪПРОСА

Кои български сектори са назовани в криминални, политически и официални източници през 2026 г. и каква реакция изисква всеки от тях?

9

сектора с наблюдавана активност, от държавната администрация до селското стопанство

НАКРАТКО

Публикациите и докладите по-долу показват как престъпници, хактивисти и власти описват активността срещу български организации през 2026 г. Повечето примери от тъмната мрежа са твърдения; редовете цитират и официални доклади, отбелязани с раздела си. Застраховането, държавната администрация и телекомите събраха най-конкретните твърдения, а банковият сектор събра най-много инструменти за измами. Проверете всяко твърдение със засегнатата организация преди ескалация и започнете с първата реакция за сектора.

Жертвите са описани по роля съгласно политиката в **Приложение** A.9.

Държавна администрация (шпионаж и поща)

`Шпионаж` `имейли със заплахи`

ПРИМЕР ЗА НАБЛЮДАВАНА АКТИВНОСТ (АНОНИМИЗИРАН)

Официално разкрит дългогодишен неоторизиран достъп до държавните мрежи за обмен на документи (§7.2); достъп до пощенски кутии на местни служители според изследователи, цитирани от Reuters (§7.2); имейли с бомбени заплахи от отвлечени акаунти (§4.5)

КАКВО ОЗНАЧАВА

Пощата и обменът на документи са изложеният слой; официалната версия не съобщава за изтичане на лични данни на граждани

ПЪРВА РЕАКЦИЯ

Централизирано събиране на логове и ретроспективно търсене в пощенските и документните системи; преглед на влизанията на администраторите на пощата

Държавна администрация (твърдения и прекъсвания)

`Твърдения за достъп` `съобщение за прекъсване`

ПРИМЕР ЗА НАБЛЮДАВАНА АКТИВНОСТ (АНОНИМИЗИРАН)

Твърдение във форум за „правителствени данни" дни след първото разкритие (случай B); правителствен пощенски панел за 10 USD (случай C); два държавни сайта, съобщени като недостъпни в изборния ден (§6.3); публикувани мрежови адреси на държавна система в транспортния сектор (§4.5)

КАКВО ОЗНАЧАВА

Твърденията не са потвърдени; причината за прекъсването остава открита

ПЪРВА РЕАКЦИЯ

Проверка на твърденията преди коментар; предварително съгласувани изявления за състоянието на услугите (§6.6)

Застраховане

`Твърдения за данни` `уведомления за нарушение` `обяви за изнудване`

ПРИМЕР ЗА НАБЛЮДАВАНА АКТИВНОСТ (АНОНИМИЗИРАН)

Поне три оферти за данни на застрахователни клиенти (август–септември) и уведомления за нарушение от три застрахователни дружества от две групи, потвърдени от регулатора (случай A); застраховател и неговото холдингово дружество на сайт за изтичане на рансъмуер (юли, §7.4)

КАКВО ОЗНАЧАВА

Рекламирани данни за самоличност на клиенти с ЕГН; автентичността не е проверена

ПЪРВА РЕАКЦИЯ

Сравняване на образците със схемите за експорт; преглед на достъпа до портала и до API на партньорите

Банки и плащания

`Сметки на „муле“` `кардинг` `твърдение за достъп` `фишинг`

ПРИМЕР ЗА НАБЛЮДАВАНА АКТИВНОСТ (АНОНИМИЗИРАН)

Сметки с български IBAN, купувани и продавани за 40–250 USD; купувач, който изброява девет български банки (§8.1); резултати от проверка на карти с 15 издатели (§8.2); твърдян достъп до портал за разработчици на банка (случай F); арести по случая Smishing Triad (§7.7)

КАКВО ОЗНАЧАВА

Преобладават инструментите за измами; експозицията, важна за проникване, е в данните за устройства и обяви (глава 9)

ПЪРВА РЕАКЦИЯ

Приоритизиране на актуалните обяви, след това на устройствата на служителите; сигнали при отказ от BIN проверки

Телекоми и интернет услуги

`Списъци с идентификационни данни` `обява за изнудване` `инцидент` `оповестен от компания`

ПРИМЕР ЗА НАБЛЮДАВАНА АКТИВНОСТ (АНОНИМИЗИРАН)

Списъци с „валидни“ и „cracked and inboxed“ акаунти за водеща българска уебпоща и инструменти за проверката им (случай D); обява за рансъмуер срещу компания за интернет услуги (§7.4); неоторизиран достъп до клиентската система на голям хостинг доставчик, оповестен от него (ноември, §7.6)

КАКВО ОЗНАЧАВА

Данни за лична уебпоща се търгуват всеки месец и се използват повторно в работни системи

ПЪРВА РЕАКЦИЯ

Блокиране на личната уебпоща за корпоративни регистрации; задължително MFA

Търговия на дребно и електронна търговия

`Твърдения за данни` `обяви за изнудване`

ПРИМЕР ЗА НАБЛЮДАВАНА АКТИВНОСТ (АНОНИМИЗИРАН)

База данни на онлайн търговец с „около 4M записа“ (февруари); клиентски данни на търговец на мебели, съобщени като продавани (февруари); търговско дружество и аптечна верига на сайтове за изтичане (§7.4)

КАКВО ОЗНАЧАВА

Клиентските контакти подхранват фишинг с тематика поръчки

ПЪРВА РЕАКЦИЯ

Проверка на масовите експорти и API логовете; предупреждение към клиентите

Здравеопазване

`Твърдение за данни` `обява за изнудване`

ПРИМЕР ЗА НАБЛЮДАВАНА АКТИВНОСТ (АНОНИМИЗИРАН)

База данни на здравна платформа, предложена два дни след твърдяната дата на пробива (януари, случай E); аптечна верига на сайт за изтичане (септември)

КАКВО ОЗНАЧАВА

Данните от здравни платформи добавят дати на раждане и контакти към измамите със самоличност

ПЪРВА РЕАКЦИЯ

Преглед на логовете за експорт и на администраторския достъп до платформата

Медии

`Уеб проникване (с повдигнато обвинение)` `твърдение за DDoS`

ПРИМЕР ЗА НАБЛЮДАВАНА АКТИВНОСТ (АНОНИМИЗИРАН)

Сайтовете на обществените медии БНТ и БНР, посочени от прокуратурата сред сайтовете, до които заподозрян е имал достъп (октомври, §7.7); спортен новинарски портал в твърдение за DDoS (март, §6.2)

КАКВО ОЗНАЧАВА

Медийните сайтове съхраняват бази данни с абонати и контакти и са символни цели

ПЪРВА РЕАКЦИЯ

Обновяване на системата за управление на съдържанието (CMS); наблюдение на експортите от базите данни

Транспорт и логистика

`Обява за изнудване` `представяне за друго лице` `твърдение за разузнаване`

ПРИМЕР ЗА НАБЛЮДАВАНА АКТИВНОСТ (АНОНИМИЗИРАН)

Логистична фирма на сайт за изтичане (юли, §7.4); SMS фишинг от името на куриери (§8.5); публикувани мрежови адреси на държавна система в транспортния сектор (§4.5)

КАКВО ОЗНАЧАВА

Куриерите се повтарят в съобщените SMS фишинг кампании

ПЪРВА РЕАКЦИЯ

Публикуване на официалните идентификатори на подателя; искане за сваляне на имитиращи домейни

Селско стопанство и съоръжения

`Твърдения за достъп до OT и устройства`

ПРИМЕР ЗА НАБЛЮДАВАНА АКТИВНОСТ (АНОНИМИЗИРАН)

Панел на оператор на оранжерии, контрол над който твърди Z-Pentest, посочена в съвместно предупреждение сред пророските хактивисти (октомври, §6.4); предложени данни за вход в 140 камери (август, случай F)

КАКВО ОЗНАЧАВА

Слабо защитените, достъпни от интернет панели и камери са цел на опортюнистични твърдения за достъп

ПЪРВА РЕАКЦИЯ

Премахване на паролите по подразбиране; извеждане на интерфейсите за управление извън интернет

Прочит по сектори. Твърденията, насочени към конкретни организации, се делят на три групи. Продавачите на данни назовават застрахователи, търговци и здравни платформи и твърдят, че имат клиентски бази данни. Рансъмуер групите назовават средни по размер компании от различни сектори. Политическите участници в нашите данни отправят малко твърдения срещу България. Най-значимата активност на държавно ниво е съобщена от самото правителство, а не е заявена от някого.

ОСНОВНИ ИЗВОДИ

01

Застраховането събра най-значимите твърдения за данни през годината, а регулаторът потвърди уведомления за нарушение от три застрахователни дружества от две групи.

02

Експозицията на държавната администрация е в пощата и обмена на документи, а не в твърдени бази данни на населението.

03

За банките и телекомите в публикациите преобладават инструменти за измами и списъци с идентификационни данни; експозицията, важна за проникване, е в данните за устройства и обяви (глава 9).

ГЛАВА 6

Хактивизъм, DDoS и твърдения за смущения

ТАЗИ ГЛАВА ОТГОВАРЯ НА ВЪПРОСА

Кой обяви смущения срещу България през 2026 г., какво казаха институциите и как организацията да се подготви за следващото твърдение?

2

набора хактивистки твърдения в нашите данни, и двата препубликувани от трети страни

В ТАЗИ ГЛАВА

6.1 Хронология | 6.2 Твърденията за DDoS през март | 6.3 Изборният ден, 19 април | 6.4 Твърдение за операционни технологии | 6.5 Какво не видяхме | 6.6 Уроци за защитниците

НАКРАТКО

Хактивистките твърдения срещу България в нашите данни за 2026 г. са малко. През март има две твърдения за DDoS с послание за Газа, а през октомври твърдение на Z-Pentest за контрол над панел за управление на оранжерия. Всички са видени чрез препубликуване. В изборния ден през април министерството първо не съобщи за атаки за отказ на услуга; по-късно медии съобщиха, че два държавни сайта са били недостъпни с часове. Договорете предварително кой потвърждава състоянието на услугите и изведете контролните панели от интернет.

6.1 Хронология

5 мар 2026 — **TheGarudaEye**
Твърди, че сайт на министерство е „down", с линк към проверка на достъпността и послание за Газа; препубликувано от канал с линкове към onion сайтове

6 мар 2026 — **TheGarudaEye**
Твърди, че спортен новинарски портал е „down", със същото послание

16 апр 2026 — **Министерство на вътрешните работи (МВР)**
Звеното за киберпрестъпност е участвало (13 април) в операция на Европол срещу DDoS услуги под наем. Резултати: идентифицирани над 75 000 потребители, 4 ареста, закрити 53 домейна

19 апр 2026 — **Министерство на електронното управление**
Изборен ден: следобед не се съобщава за засилена кибернетична активност срещу стратегически обекти, нито за атаки за отказ на услуга

19 апр 2026 — **Медии (News.bg, позовавайки се на Нова)**
Сайтовете на министерството и на Министерския съвет са съобщени като недостъпни след кибератака; възстановени малко след 19:00

7 юли 2026 — **Медии (БНР)**
Имейли със заплахи за бомби в продължение на два дни. Първата вълна достигна до съдилища, прокуратури и общини в над 22 града; на втория ден се добавиха болници и данъчни служби. Разследващите го определят като „автоматизирана хибридна атака"

9 юли 2026 — **CERT България**
Имейли със заплахи за бомби, изпращани до държавни институции от отвлечени акаунти от 6 юли

17 сеп 2026 — **ДАНС**
Допълнителни указания за киберсигурност за всички стратегически обекти преди изборите на 25 октомври

14 окт 2026 — **Z-Pentest / Z-Alliance**
Твърди, че контролира панел за автоматизация на оранжерия в България и че е преименувал устройството; препубликувано от испаноезичен канал

Тъмните маркери са публикации на участници, контурните маркери са препубликувания от трети страни, кораленните маркери са официални изявления. Датите са на публикацията или изявлението; софийското време е UTC+2 (UTC+3 през лятото).

6.2 Твърденията за DDoS през март

На 5 март канал, който препубликува линкове към onion сайтове, препредаде публикация със заглавие „GLOBAL CYBER ATTACK #0070". В нея се твърди, че сайтът на българско министерство е „DOWN by TheGarudaEye" в 08:36 местно време, с линк към проверка на достъпността като доказателство. Посланието критикува международни планове за Газа. На 8 март същият канал препубликува второ твърдение, срещу спортен новинарски портал, с дата 6 март [S1].

КАРТА НА ПУБЛИКАЦИЯ B10 — 5 мар 2026

TheGarudaEye (relayed)

Telegram канал с onion връзки, препредаващ твърдение · Telegram · английски

ОРИГИНАЛ

```
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? [...]
```

ПРЕВОД

ГЛОБАЛНА КИБЕРАТАКА #0070
Цел: [българско министерство]
СВАЛЕНО от TheGarudaEye
Сървърът е свален: 05/03/2026 (08:36 българско време)
Доказателство: [връзката към проверка на достъпността е премахната]
Съобщение: Изграждане на нова Газа без участието на хората от Газа и Палестина? [...]

Бележка. Останалата част от съобщението е политическа реторика на извършителя и е пропусната.

КАКВО МОЖЕМ ДА УСТАНОВИМ	Твърдението, неговият час и неговата рамка.
КАКВО НЕ Е УСТАНОВЕНО	Прекъсване, неговата причина или продължителност; че извършителят е изпратил какъвто и да е трафик.

Какво можем да установим. Че твърденията са публикувани и препубликувани. Линкът към проверка на достъпността може най-много да запише момент на недостъпност от някои тестови локации. Той не показва прекъсване, неговата причина или продължителност. Не открихме официално изявление за нито един от двата сайта. Рамката засяга събития извън България; България е една от целите в номерирана поредица.

6.3 Изборният ден, 19 април

В изявление, съобщено в 16:12, министерството, което тогава отговаряше за електронното управление, заяви, че няма засилена кибернетична активност срещу стратегически обекти и няма атаки за отказ на услуга. Временен ситуационен център по киберсигурност работеше от 08:00 до полунощ [S18]. По-късно същия следобед News.bg, позовавайки се на телевизия Нова, съобщи, че сайтовете на

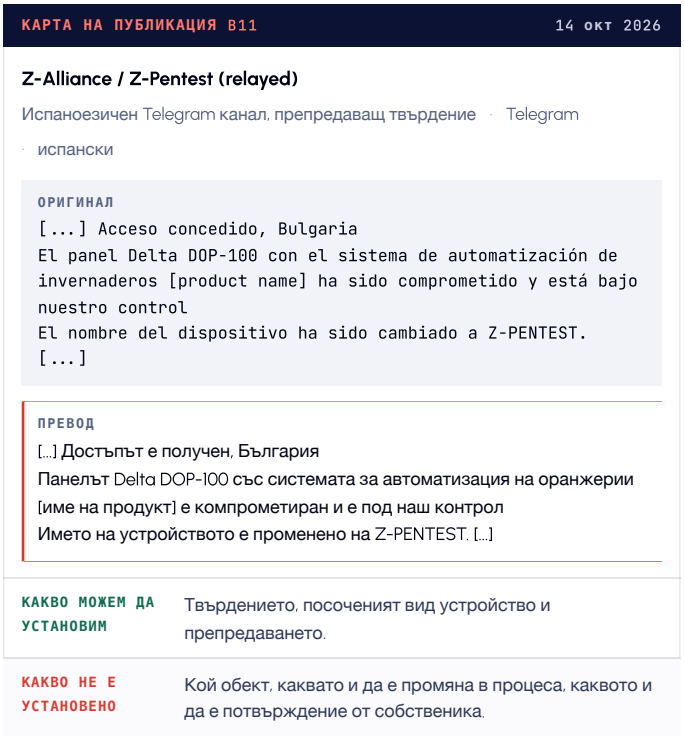
министерството и на Министерския съвет са изгубили свързаност след кибератака. Министерството заяви, че въпреки прекъсването системите му работят нормално. Сайтовете бяха възстановени малко след 19:00 [S19].

Аспект	Медийна информация	Официална версия	Какво остава открито
Ефект	Два държавни сайта без свързаност с часове [S19]	Системите „функционират нормално" въпреки прекъсването [S19]; по-рано същия ден не се съобщава за атаки за отказ на услуга [S18]	Дали прекъсването е причинено от атака или от проблем със свързаността
Обхват	Сайтовете на министерството и на Министерския съвет; сайтът на МВР е труден за достъп при собствената проверка на медията [S19]	Няма списък на засегнатите сайтове	Други сайтове
Приписване	Няма	Няма	Участник и метод
Последваща оценка	Не е посочена	Само ограничени кибератаки в последните часове на изборния ден, според служебен заместник-министър през май [S20]	Не е публикуван технически доклад

Какво означава това. В ден на максимално обществено внимание два държавни сайта бяха съобщени като недостъпни за няколко часа. Официалната версия и медиите го описаха с различни думи. В нашите данни нито един участник не пое отговорност. Защитният урок е същият като при всяко твърдение за DDoS: една предварително договорена публична позиция, дадена рано.

6.4 Твърдение за операционни технологии

На 14 октомври испаноезичен канал за препредаване препубликува твърдение на „Z-Alliance" и Z-Pentest, група, която съвместното предупреждение от декември 2025 г. посочва сред пророските хактивисти [S68]. Според него операторски панел марка Delta, управляващ система за автоматизация на оранжерия в България, е „под наш контрол". Името на устройството е било сменено на Z-PENTEST [S1].



Какво можем да установим. Твърдението, посочения в него тип устройство и препубликуването. Ние не сме го проверили и доколкото открихме, нито собственикът, нито институция са го потвърдили. Подобни твърдения обикновено засягат достъпни от интернет операторски панели с пароли по подразбиране или без пароли. Те са евтини за заявителя и потенциално скъпи за собственика. През

ноември CERT България предупреди за атаки в Европа срещу достъпни от интернет контролери на хладилни системи [S37], което сочи същата слабост.

Отделно доставчик на разузнаване за заплахи съобщи за твърдение от 2026 г. на AlfaNet или Z-Pentest Alliance. Твърдението е за пълен контрол над сървър Rapid SCADA (система за надзорно управление и събиране на данни), свързан с енергийната и газовата инфраструктура в България; доставчикът го представи като твърдение на групата [S69].

6.5 Какво не видяхме

Не открихме твърдение от 2026 г. срещу български цели от най-активните в Европа DDoS групи от последните години извън описаните по-горе. В нашите данни има логове от стрес тестове с български хостинг диапазони, но те записват тестов трафик, а не обявени кампании.

Отсъствието от нашата колекция не означава отсъствие на атаки. Твърденията в затворени канали и атаките, за които никой не поема отговорност, тук са невидими.

Повторно търсене в публичните източници на английски, български, руски и турски език не откри надежден доклад за хактивистка DDoS кампания срещу български цели през 2026 г. На 19 ноември министърът заяви, че атаките срещу правителствени сайтове продължават и се блокират, без да назове заявител [S61].

6.6 Уроци за защитниците

1. **Договорете предварително публичната позиция.** В изборния ден медиите и министерството описаха едно и също прекъсване по различен начин. Решете предварително кой потвърждава състоянието на услугите, в какъв срок и по какъв канал.
2. **Защитете порталите на ниво доставчик.** Порталите за граждани се нуждаят от договорена защита срещу DDoS преди избори или значима дата, а не по време на тях.
3. **Изведете операторските панели от интернет.** Контролерите на оранжерии, хладилни системи, сгради и камери трябва да са зад VPN и с идентификационни данни, различни от фабричните.
4. **Очаквайте заплашителни имейли от реални пощенски кутии.** Юлските имейли със заплахи за бомби дойдоха от отвлечени акаунти, които преминаха проверките за автентичност на пощата [S35]. Първата вълна достигна до съдилища, прокуратури и общини в над 22 града, а след това болници и данъчни служби [S72]. Обучете служителите и осигурете канал за докладване.

ОСНОВНИ ИЗВОДИ

01

Хактивистките твърдения срещу България в нашите данни за 2026 г. са малко и нито едно не е потвърдено от засегнатата организация или институция.

02

В изборния ден два държавни сайта бяха съобщени като недостъпни с часове, докато министерството заяви, че системите му работят нормално; предварително договорената публична позиция затваря тази разлика.

03

Слабо защитените, достъпни от интернет панели са цел на опортюнистични твърдения за достъп.

ГЛАВА 7

Участници на заплахи

07

19

вписвания на рансъмуер групи в сайтове за изтичане за България през 2026 г. след преглед, назоваващи 17 организации

ТАЗИ ГЛАВА ОТГОВАРЯ НА ВЪПРОСА

Кой стои зад активността, как са свързани участниците и какво казва официалната информация за всеки от тях?

В ТАЗИ ГЛАВА

7.1 Как са свързани участниците · 7.2 Шпионаж срещу държавни мрежи · 7.3 Хактивисти и заявители на смущения · 7.4 Рансъмуер и изнудване · 7.5 Престъпни персони, видени в Blackhole · 7.6 Инцидент, оповестен от компания · 7.7 Официално съобщени операции и арести

НАКРАТКО

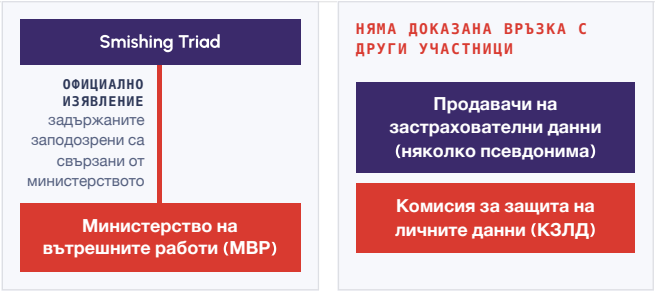
За България през 2026 г. значение имат пет типа участници. Според правителството неидентифицирана операция по проникване е продължила години в държавните мрежи за обмен на документи. Рансъмуер групи публикуваха 19 вписвания за 17 български организации, при 7 през 2025 г.; покритието се променя, затова това не е темп на растеж. Престъпни продавачи търгуват с български данни за самоличност, акаунти и идентификационни данни. Хактивистите са обявили малко. Полицейските случаи добавят фишинг и измамни мрежи, някои международни. Първо търсете дълготраен достъп в пощенските и документните системи, после упражнете сценарий за изнудване.

Всеки профил разделя **наблюдаваното поведение**, **собственото твърдение на участника**, **неизяснените въпроси** и **значението за организациите**. Степента на увереност се отнася за конкретна теза, а не за участника като цяло.

7.1 Как са свързани участниците

Картата свързва участниците само там, където имаме доказателства, и всяка линия посочва вида им: препубликуване от трета страна, официално изявление или наши собствени данни. Линията е връзка, а не доказателство за общ оператор.





Твърдението „Starred Bears" във форума (случай B) се появи дни след първото разкритие; нищо не го свързва с проникването, затова картата не чертае линия между тях. Три застрахователни дружества от две групи са уведомили органа за защита на данните за пробиви (§4.4); нито една оферта не е съпоставена с някое от уведомленията, затова и там картата не чертае линия.

7.2 Шпионаж срещу държавни мрежи

Неидентифицирано шпионско проникване

Няма публично име

Кибершпионаж (официално съобщен)

Не е приписано; министърът заяви, че се смята, че са замесени няколко международни хакерски групи и че не е открита категорична връзка с държава

В БЪЛГАРИЯ, 2026

5 август	Министерството съобщава за неоторизиран достъп до административни мрежи, възможно продължил години
18 ноември	Министерството заявява, че достъпът от 2021 г. до държавната инфраструктура за обмен на документи е прекъснат на три фази
18 ноември	Министърът посочва най-малко 130 GB, над 62 милиона страници; министърът заявява, че прокуратурата е сезирана да провери действията на държавните органи през този период

ЗАЯВЕНИ ЦЕЛИ

Инфраструктурата, чрез която държавните институции обменят документи и информация

В ПУБЛИЧНИ ИЗТОЧНИЦИ

- [S22] Министерство на иновациите и дигиталната трансформация: неоторизиран достъп, открит при внедряването на националната система за киберсигурност
- [S23] Министерството: достъп от 2021 г.; засега не е установено излагане на личните данни на гражданите; засилено наблюдение за 90 дни
- [S24] Mediapool: според министъра мотивите и връзките на групите са неизвестни; няма информация документите да са се появили в тъмната мрежа
- [S25] Reuters: няма категорични доказателства, които да свързват нападателите с конкретна държава

НАШАТА ОЦЕНКА

Според правителството най-значимото проникване за годината. Входният път, инструментите и участниците не са публични и нищо в нашите данни от тъмната мрежа не може да бъде свързано с него.

СТЕПЕН НА УВЕРЕНОСТ **Висока, че правителството съобщава за проникване, продължило години; участникът и методът са неизяснени**

Версията на правителството е единственият публичен източник за това проникване и тя е представяна на етапи. На 5 август министерството заяви, че е открило неоторизиран достъп до определени административни мрежи при внедряването на новата национална система за киберсигурност [S22]. На 18 ноември то заяви, че достъпът е продължавал от 2021 г. и е засягал инфраструктурата, чрез която институциите обменят информация. Според министерството нападателите са били прекъснати и отстранени на три фази, а засегнатата инфраструктура ще остане под засилено наблюдение 90 дни [S23].

На брифинг същия ден министърът посочи обем от най-малко 130 GB, над 62 милиона страници, обхващащи повечето области на държавната администрация. Той заяви, че се смята, че са замесени няколко международни хакерски групи. Според него не е установено дали те са действали самостоятелно, заедно или за чужди разузнавателни служби. Той няма информация документите да са се появили в тъмната мрежа [S24][S25]. Министърът заяви, че прокуратурата е сезирана да провери действията на държавните органи през този период [S25].

Неизяснено. Входният път, инструментите, участниците и дали данни са били използвани. **Значение.** Според правителството слой за обмен на документи е бил четим около пет години; министърът заяви, че новата национална система за първи път дава единна картина [S24]. За всяка организация, която обменя документи с държавата, решаващите контроли са централизираното журналиране, контролът над администраторските акаунти и търсенето на дълготраен достъп, а не алармите по периметъра. Нищо в нашите данни от тъмната мрежа за 2026 г. не може да бъде свързано с това проникване (случай B, §4.6).

Други публикации за шпионаж през 2026 г., които назовават България. Още две публикации засягат български цели, като при всяка приписването е това, което посочва източникът.

Дата	Съобщено от	Какво казва източникът	Приписване според източника
15 април	Reuters, препубликувано от Fakti	Изследователи са намерили на сървър на нападателите следи от достъп до поне четири пощенски кутии на местни служители в Пловдивска област, в кампания с поне 284 кутии (септември 2024 г.–март 2026 г.); българските власти не са отговорили [S67]	Изследователите я приписват на Fancy Bear (APT28); ESET не е могла да потвърди това, а втори доставчик го оспорва [S67]
4 ноември	Sekoia; съобщено от Ruse.news на 5 ноември	Сайт от военния сектор на България е бил един от няколкото сайта, в които нападателите са подменили JavaScript библиотека, за да насочват телефоните на посетителите към експлойти за вече отстранени (n-day) уязвимости. Sekoia не посочва дали някой посетител е бил атакуван [S66]	APT29, със средна до висока степен на увереност, според Sekoia [S66]

Значение. И двата случая достигат до хората чрез инструменти, на които те имат доверие: пощенска кутия в уеб поща и познат сайт, отворен на телефон. Наблюдението на пощенските акаунти, MFA, устойчиво на фишинг, и навременните обновления на мобилните устройства са контролите, към които сочат тези доклади.

7.3 Хактивисти и заявители на смущения

TheGarudaEye

Хактивист (твърдения за DDoS)

Рамка за Газа в собствените му съобщения; не открихме надежден публичен профил

В БЪЛГАРИЯ, 2026

5 март	Твърди, че сайт на министерство е недостъпен (B10)
6 март	Твърди, че спортен новинарски портал е недостъпен

ЗАЯВЕНИ ЦЕЛИ

Сайт на министерство и спортен новинарски портал

С ТЕХНИТЕ ДУМИ

> *"GLOBAL CYBER ATTACK #0070"* B10

В ПУБЛИЧНИ ИЗТОЧНИЦИ

НАШАТА ОЦЕНКА

Номерирана поредица от твърдения, в която България е една от целите; доказателствата са линкове към проверка на достъпността. Не открихме надеждни публични материали за групата.

СТЕПЕН НА УВЕРЕНОСТ **Висока, че твърденията са публикувани и препубликувани; ефектът не е проверен**

Z-Pentest

Представя се като част от „Z-Alliance"

Хактивист (твърдения за достъп до OT)

Посочена сред пророските хактивистки групи в съвместното предупреждение AA25-343A [S68]

В БЪЛГАРИЯ, 2026

14 октомври Твърди, че контролира панел за автоматизация на оранжерия в България (B11)

ЗАЯВЕНИ ЦЕЛИ

Достъпен от интернет операторски панел на търговска оранжерия

С ТЕХНИТЕ ДУМИ

> *"Acceso concedido, Bulgaria"* B11

В ПУБЛИЧНИ ИЗТОЧНИЦИ

- [S68] Съвместно предупреждение AA25-343A (декември 2025 г.): посочена сред проруските хактивистки групи, които използват слабо защитени, достъпни от интернет VNC връзки (отдалечен работен плот), за да достигнат до контролни устройства в ОТ
- [S69] KELA (2026 г.): AlfaNet или Z-Pentest Alliance твърди, че контролира сървър Rapid SCADA, свързан с енергийната и газовата инфраструктура в България; представено като твърдение на групата

НАШАТА ОЦЕНКА

Препубликувано твърдение за операторски панел, съвместимо със съобщавания фокус на групата върху достъпни от интернет ОТ системи. Българските ѝ твърдения не са потвърдени от засегнатата организация или институция.

СТЕПЕН НА УВЕРЕНОСТ **Висока, че твърдението е препубликувано; достъпът не е проверен**

Дейността на нито един от двамата заявители срещу България не е потвърдена от засегнатата организация или институция. Съвместното предупреждение AA25-343A е издадено през декември 2025 г. от CISA, ФБР и международни партньорски агенции. То посочва Z-Pentest сред проруските хактивистки групи, които достигат до операционни технологии чрез слабо защитени, достъпни от интернет връзки за отдалечен достъп (VNC) [S68]. Не открихме надежден публичен профил на TheGarudaEye. Прекъсването на два държавни сайта в изборния ден (§6.3) не е обявено от нито един участник в нашите данни.

7.4 Рансъмуер и изнудване

Ransompedia съдържа 19 български вписвания през 2026 г., близо до Румъния и Гърция и значително над Сърбия и Северна Македония

БЪЛГАРИЯ

19

Обяви след преглед, 1 яну-18 ное 2026

2025	ЗА ЦЕЛИЯ ПЕРИОД
7	52

ГРУПИ ПРЕЗ 2026 Г.
N0n, NightSpire, The Gentlemen, Krybit, Everest, Vexy-ransomware, Braincipher, MedUSlocker, Panzer, Majinahanashi, Deadlock, 0day-syndicate, LockBit 5, Anubis

РУМЪНИЯ

20

Обяви след преглед, 1 яну-18 ное 2026

2025	ЗА ЦЕЛИЯ ПЕРИОД
17	65

ГРУПИ ПРЕЗ 2026 Г.
Qilin, LockBit 5, The Gentlemen, RansomHouse, Deadlock, INC Ransom, Nova, Lamashtu, Krybit, 0apt, Lynx, Kill Security

ГЪРЦИЯ

19

Обяви след преглед, 1 яну-18 ное 2026

2025	ЗА ЦЕЛИЯ ПЕРИОД
19	62

ГРУПИ ПРЕЗ 2026 Г.
The Gentlemen, Settra, DragonForce, INC Ransom, LockBit 5, Deadlock, Global-secret-group, Blacknevas, Coinbasecartel, Alphalocker, MyData, Qilin, NightSpire

СЪРБИЯ

7

Обяви след преглед, 1 яну-18 ное 2026

2025	ЗА ЦЕЛИЯ ПЕРИОД
1	17

ГРУПИ ПРЕЗ 2026 Г.
APT73, LockBit 5, The Gentlemen, Panzer, INC Ransom

СЕВЕРНА МАКЕДОНИЯ

3

Обяви след преглед, 1 яну-18 ное 2026

2025	ЗА ЦЕЛИЯ ПЕРИОД
1	9

ГРУПИ ПРЕЗ 2026 Г.
The Gentlemen, INC Ransom, APT73

Източник: обяви в Brandefense Ransompedia след преглед, всички дати, до 18 ноември 2026 г. [S6]; ransomware.live за кръстосана проверка [S7].

След преглед Ransompedia съдържа 19 вписвания на български организации между 1 януари и 18 ноември 2026 г., при 7 за цялата 2025 г. и 52 общо. Две организации са вписани по два пъти, така че 19-те вписвания назовават 17 организации. Румъния има 20 вписвания за същия период, Гърция 19, Сърбия 7 и Северна Македония 3 [S6]. Вписванията са през януари (3), май (2), юли (5), септември (5) и октомври (4).

Показател	Стойност за 2026 г.
Групи	14, водени от Krybit, N0n, NightSpire, The Gentlemen и Everest с по две вписвания всяка
Сектори (етикети на Ransompedia)	Образование 3, финанси 2, здравеопазване 2, развлечения 2, технологии 2; по едно в търговията на дребно, медиите, ИТ услугите, логистиката, храните и напитките и хотелиерството; две с други или междусекторни етикети
Обявени организации по роля (примери)	Холдингово дружество и застрахователното му дъщерно дружество (юли, една група, с един ден разлика). Търговско дружество; производител на гейминг технологии; аптечна верига; доставчик на офис техника; компания за интернет услуги
Непреброени твърдения	Три препубликувани или тракерни твърдения не са преброени след преглед, включително едно, което публичен тракер [S7] отбелязва като българско, а Ransompedia води като сръбско

Krybit

Рансъмуер и изнудване с данни | Финансово мотивиран

В БЪЛГАРИЯ, 2026

юли	Вписва застрахователна компания в сайта си за изтичане
юли	Вписва холдинга майка на застрахователя (B18)

ЗАЯВЕНИ ЦЕЛИ

Холдингово дружество и застрахователното му дъщерно дружество

С ТЕХНИТЕ ДУМИ

> *"krybit claims attack"* B18

В ПУБЛИЧНИ ИЗТОЧНИЦИ

- [S6] Ransompedia: две български вписвания през 2026 г., и двете през юли; едно румънско вписване за същия период
- [S70] Cyble: финансово мотивиран рансъмуер като услуга, изграден върху изтекъл код на Babuk, наблюдаван за първи път през март 2026 г.; България не се споменава

НАШАТА ОЦЕНКА

Единствената група с две български вписвания от една и съща корпоративна група. Вписванията са твърдения; доколкото открихме, към крайната дата нито една от двете компании не е потвърдила инцидент.

СТЕПЕН НА УВЕРЕНОСТ **Висока, че вписванията съществуват; проникване не е проверено**

КАРТА НА ПУБЛИКАЦИЯ B18 — 19 юли 2026

Leak-monitor bot

Telegram бот за наблюдение на изтичания, препредаващ тракер за рансъмуер

Telegram · английски

ОРИГИНАЛ

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

ПРЕВОД

"Victim": "[холдингово дружество]",
"Content": "Рансъмуер групата krybit поема отговорност за атака срещу [холдингово дружество]. [...]"
"Type": "Ransom Alert"

Бележка. Същата група обяви и застрахователното дъщерно дружество на холдинга (§7.4).

КАКВО МОЖЕМ ДА УСТАНОВИМ	Че групата е обявила холдинга на своя сайт за изтичане, според препредаването.
КАКВО НЕ Е УСТАНОВЕНО	Каквото и да е проникване, криптиране или кражба на данни; каквито и да е преговори.

Cyble описва Krybit като финансово мотивирана операция за рансъмуер като услуга, изградена върху изтекъл код на Babuk и наблюдавана за първи път през март 2026 г.; профилът на Cyble не споменава България [S70].

Какво означава това. Вписването е твърдение на престъпник, че притежава данни и че жертвата не е платила. То не е доказателство за пробив или криптиране. Доколкото открихме, към крайната дата нито една от 17-те организации не е потвърдила инцидент. Броят за 2026 г. е висок спрямо предходната година, но покритието на Ransompedia и поведението на групите се променят. Затова не го тълкуваме като темп на растеж.

Броят все пак показва, че рансъмуер групите публикуват български организации в брой, сравним с Румъния и Гърция. През юли министърът на вътрешните работи също посочи рансъмуер срещу фирмени мрежи сред заплахите, които полицията вижда [S38]. За 2025 г. агенцията на ЕС за киберсигурност ENISA причислява България към най-малко атакуваните държави членки, с 0,3% от твърденията за рансъмуер в ЕС [S64]. Вписванията за 2026 г. стоят на фона на тази ниска база.

7.5 Престъпни персони, видени в Blackhole

Само псевдоними; без контакти, линкове или реални самоличности.

Персона или марка	Наблюдавана роля през 2026 г.	Собствено твърдение	Неизяснено
thejackal101	Публикува комболистове в няколко форума; списъци „Database: Bulgaria" (януари-октомври)	68 000-126 000 „пресни" реда на списък	Произход, припокриване, валидност (случай D)
Max_Leaks / Maxleak	Марка за комболистове в два форума (април-септември)	56 000-150 000 реда на списък	Както по-горе
kookiegst	Публикува списъци с „попадения" за уеб поща (август)	Акаунти, „току-що разбити и с проверен достъп до пощата"	Валидност
DuperKinger123	Продавач във форум на панели за правителствена поща на няколко държави (април)	Панел за поща на българското правителство, 10 USD	Каквато и да е проверка (случай C)
lauraallen	Продавач във форум на „Bulgaria insurance database" (септември)	Примерен заглавен ред с ЕГН	Произход (случай A)

Персона или марка	Наблюдавана роля през 2026 г.	Собствено твърдение	Неизяснено
Intelligence	Нов акаунт във форум, предложил данни, приписвани на застраховател, според медиите (септември)	3,1 милиона реда	Каквато и да е проверка [S32]
Enigma Group	Публикува мрежови адреси на държавна система в транспортния сектор (август)	Адреси на бекенд VPN и WAN	Какъвто и да е достъп
Commando	Продавач на администраторски акаунт за уебсайта на компания за събития (февруари)	Администраторски достъп, 50 EUR	Каквато и да е проверка
X FORUMS (бот)	Автоматично качва малки файлове с идентификационни данни, включително за български домейни	Няма	Не е човек; бот за разпространение

7.6 Инцидент, оповестен от компания

На 17 ноември голям български хостинг доставчик заяви, че е открил неоторизиран достъп до една от вътрешните си системи, съобщи Money.bg. Засегнати са данни от клиентските профили: имена, имейл адреси, телефонни номера и данни за фактуриране, включително ЕГН или ЕИК. Компанията заяви, че хостинг услугите не са засегнати, паролите се съхраняват хеширани и част от тях са сменени превантивно. Според нея досега няма индикации за изтичане на клиентски данни. Компанията е уведомила КЗЛД и CERT България [S65]. Управителят ѝ заяви, че атаката вероятно е извършена от автоматизиран ИИ агент; това е собствената оценка на компанията [S65].

Значение. Клиентската база данни на хостинг доставчик назовава хората, които администрират хиляди български сайтове. Клиентите му трябва да очакват фишинг, който цитира реалните данни на акаунтите им, и да включат MFA за хостинг акаунтите си.

7.7 Официално съобщени операции и арести

Публикациите показват оферти; официалната информация показва арести на хора. Пет случая от 2026 г. се открояват, защото посочват метода.

Дата	Съобщено от	Какво се е случило
14 март	МВР	Служители на дирекция „Киберпрестъпност" задържаха двама чужди граждани, купували смартфони в София с чужди платежни карти; министерството заяви, че е установено участието им в международната група „Smishing Triad" [S39]
16 април	МВР	Дирекция „Киберпрестъпност" участва (13 април) в координирана от Европол операция срещу услуги за DDoS под наем в 20 държави: идентифицирани над 75 000 потребители, 4 ареста, закрити 53 домейна [S56]
6-21 април (задържания на 9 май)	МВР	Установени са изпращачите на десетки хиляди фишинг съобщения от името на министерството, други институции и куриерски фирми; те са използвали ИИ и азиатска платформа, за да ги генерират и изпращат; двама души са задържани [S41]
28-30 октомври	Прокуратура на Република България	19-годишен е обвинен в неоторизиран достъп до сайтовете на държавни и общински институции, фирми и две национални обществени медии. Обвинението обхваща и копиране на бази данни с имена, телефонни номера, ЕГН и адреси и предлагане на данни за продажба в хакерски форуми [S42]
13 ноември	МВР	Дирекция „Киберпрестъпност" участва в операция Endgame срещу Gootloader, CastleRAT и StealC: иззети 235 сървъра и 257 домейна и идентифицирани над 6 милиона набора данни на жертви [S43]

Smishing Triad

`Мрежа за SMS фишинг`

`Финансово мотивирана; описана от МВР като международна организирана престъпна група`

В БЪЛГАРИЯ, 2026

14 март — Двама заподозрени задържани в София при покупка на смартфони с чужди карти; министерството заявява, че е установено участието им в групата

ЗАЯВЕНИ ЦЕЛИ

Притежатели на банкови карти чрез фишинг съобщения, които подвеждат жертвите да предоставят данните на картите си

В ПУБЛИЧНИ ИЗТОЧНИЦИ

- [S39] МВР: според публични данни групата действа в над 120 държави; фишинг съобщенията ѝ подвеждат жертвите да предоставят банковите си данни

НАШАТА ОЦЕНКА

Единствената международна фишинг мрежа, която българската полиция свърза по име с арест през 2026 г. Случаят свързва SMS фишинга с покупки в магазини с откраднати данни на карти.

СТЕПЕН НА УВЕРЕНОСТ **Средна: връзката е заявена от министерството; все още няма съдебно решение**

Какво казва това на защитниците. Два от петте случая са международни операции с участието на българската полиция. Другите три са срещу лица, действащи в България или от България. Случаят от октомври показва, че един участник може да достигне сайтове на държавни, общински, медийни и фирмени структури. Прокуратурата посочи двете обществени медии, БНТ и БНР, сред сайтовете. Това прави обновяването на уеб приложенията и наблюдението на експорта от бази данни контрол за държавата и медиите, а не само за електронната търговия.

ОСНОВНИ ИЗВОДИ

01

Според правителството най-значимото проникване за годината е шпионаж в държавните мрежи за обмен на документи, открит след около пет години.

02

Рансъмуер групи са публикували 19 български вписвания в брой, сравним с Румъния (20) и Гърция (19); вписванията са твърдения, а не потвърдени пробиви.

03

Полицейските случаи посочват методи, които защитниците могат да тестват: фишинг, написан с ИИ, телефони, купени с чужди карти, и уеб проникване, завършващо с продажба на данни.

ГЛАВА 8

Икономиката на измамите

ТАЗИ ГЛАВА ОТГОВАРЯ НА ВЪПРОСА

Как престъпниците превръщат българските самоличности и акаунти в пари и какво показват полицейските случаи за работещите методи?

110 USD

медианна искана цена за банков или платежен акаунт в прегледаните публикации

В ТАЗИ ГЛАВА

8.1 Търговия с банкови и платежни акаунти

8.2 Данни за карти в публикациите: тесен поглед

8.3 Самоличност, KYC и SIM услуги

8.4 Цените в контекст

8.5 Какво съобщиха полицията и надзорните органи

НАКРАТКО

Документите за самоличност и търговията с банкови и платежни акаунти са най-големите специфични за България престъпни категории в нашите данни, следвани от резултати от проверка на карти. Български IBAN, финтех акаунти и комплекти лични карти се предлагат за десетки до няколкостотин долара. Полицейските случаи от 2026 г. описват SMS фишинг от името на полицията и куриери, инвестиционни измами чрез кол центрове и, в един случай, кредит след смяна на данните за контакт в банков профил. Потвърждавайте платежните инструкции по независим канал и приемайте, че данните за самоличност са известни.

8.1 Търговия с банкови и платежни акаунти

Търговията с акаунти е второто по големина специфично за България престъпно семейство в нашите данни след документите за самоличност (291 отделни публикации срещу 341; 2 040–2 151 в прегледания маркиран набор). Купувачи и продавачи търгуват с акаунти с български IBAN в банки и платежни институции, често като „готови" или „верифицирани" акаунти. Наблюдаваните искани цени включват 40 USD за верифициран акаунт в платежна услуга (януари), 100 USD за готов акаунт в българска банка (март) и 200–250 USD за акаунти в същата банка (август–септември). Един продавач предлагаше „5–10 акаунта на ден" в друга банка (февруари). Купувач през юли изброи девет български банки, от които иска акаунти.

Рискът, който тези оферти създават за банките, не е хакване на банката, а сметки на парични мулета. Това са сметки, открити или наети с реални самоличности, които по-късно пренасят приходи от измами. Публикациите показват офертите, а не че акаунт е бил открит или използван в конкретна банка.

КАРТА НА ПУБЛИКАЦИЯ B14 12 юли 2026

mansorryuwu Telegram чат за регистрации и работа · Telegram · английски

ОРИГИНАЛ

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

ПРЕВОД

КУПУВАМ БЪЛГАРИЯ
1 [банка]
2 [банка]
3 [банка]
4 [банка]
5 [банка]
6 [банка]
[...]

Бележка. "WTB" означава "want to buy" ("купувам"). Купувачът е изброил девет български банки; имената са премахнати.

КАКВО МОЖЕМ ДА УСТАНОВИМ	Търсене на сметки в български банки.
КАКВО НЕ Е УСТАНОВЕНО	Каквато и да е открита, продадена или използвана сметка.

8.2 Данни за карти в публикациите: тесен поглед

ОБХВАТ НА ДАННИТЕ В КАРТИТЕ

Данните за карти в този доклад обхващат само платежни карти, появили се в явен текст в публикациите от тъмната мрежа, събрани за този доклад. Brandefense открива откраднати карти и чрез много други методи, които този доклад не обхваща. Тези данни не са мярка за кражбата на карти или загубите от измами в България.

В този тесен обхват в събраните публикации се появиха в явен текст 126 отделни карти, свързани с България. От тях 81 са приписани на една от 15 посочени български банки и платежни институции. Останалите 45 са обозначени само като български, без издател. 115 от тях се появиха в резултати от проверка на карти, а 114 бяха видени през януари–април [S8]. Полезният сигнал за издателите е моделът на проверка: партиди карти, тествани с малки авторизации през търговски платежни шлюзове (глава 9).

8.3 Самоличност, KYC и SIM услуги

Публикациите за KYC и документи (341 специфични за България; 1 567–1 672 в прегледания маркиран набор) предлагат верифицирани акаунти в борси и платежни услуги. Предлагат се и „лични карти от България, лице и гръб, и селфи, налични на едро" (ноември), както и услуги за изработка на изображения на документи. Купувачи търсеха български комплекти документи „на постоянна база" (септември) и български KYC (май).

През април полицията в Пловдив иззе компютър с над 1 000 сканирани български лични карти при проверки, свързани с изборите [S44]. През октомври беше рекламиран софтуер за изпращане на SMS, покриващ 32–33 държави, сред които и България. Заедно с данните за самоличност от §4.4 тези услуги намаляват цената на откриването на акаунти на чуждо име.

КАРТА НА ПУБЛИКАЦИЯ B15 — 5 ное 2026

annabelle0 · Форум за кракване · Форум · английски

ОРИГИНАЛ

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

ПРЕВОД

Български лични карти лице и гръб и селфи на едро, Telegram ПРИСЪЕДИНЕТЕ СЕ КЪМ ЧАТА ЗА ЗАОБИКАЛЯНЕ НА KYC [връзките са премахнати]

КАКВО МОЖЕМ ДА УСТАНОВИМ	Предложението.
КАКВО НЕ Е УСТАНОВЕНО	Дали документите са истински, откраднати или изфабрикувани; обемът.

8.4 Цените в контекст

Продукт (прегледани публикации)	Медианна искана цена	Разсейване
Банков или платежен акаунт	110 USD	55–230 USD
KYC или услуга за документи	100 USD	50–200 USD
Комболист	50 USD	20–400 USD
Оферта за достъп	400 USD	Широко, малко стойности
„Панел“ за правителствена поща (единична оферта)	10 USD	Единична оферта
Администраторски акаунт на уебсайт (единична оферта)	50 EUR	Единична оферта

Цените са искани цени от малцинството публикации, които посочват такава; те не измерват пазарната стойност или осъществени продажби. Разсейването е средната половина от посочените цени (от 25-и до 75-и перцентил), а не пълният диапазон.

8.5 Какво съобщиха полицията и надзорните органи

Публикациите показват оферти. Съобщенията по-долу описват опити за измами и подадени сигнали за измами; всички са публикувани през 2026 г. и нито едно не се появи в нашите данни от Blackhole.

Дата	Съобщено от	Какво се е случило
7 януари	КФН	Имейли от името на комисията съобщаваха на получателите, че за приключване на превод от чужбина е нужна допълнителна такса [S45]
23 януари	МВР	Ръст през януари на измамите срещу продавачи в сайтове за обяви: фалшив купувач изпраща фишинг линк, с който иска данни за карта и кодове за 3-D Secure; десетки сигнали [S40]
3 февруари	КФН	Управители на фирми за криптоактиви са вписани в търговския регистър с подправени документи, без знанието на собствениците, което позволява кредити на името на фирмите [S46]
8 май	МВР	Масови SMS и съобщения в приложения от името на министерството за неплатени глоби за превишена скорост „с 30% отстъпка“, с линкове към имитиращи домейни [S47]

Дата	Съобщено от	Какво се е случило
18 май; 11 ноември	CERT България	SMS фишинг, имитиращ МВР, пътната полиция и транспортното министерство за глоби и такси за паркиране, като през май са изброени близо 30 злонамерени домейна; още SMS от международни номера през ноември [S48][S49]
3 юни	МВР, според БНР	Ръководителят на отдела за киберразузнаване в дирекция „Киберпрестъпност" заяви, че три до четири български фирми седмично стават жертва на измами, при които IBAN на получателя се подменя или се получава достъп до бизнес имейл. Единичните загуби са 1–5 милиона EUR [S62]
10 юни (публикация; датата на акцията в съобщението е неясна); 21 октомври	МВР	Затворени са кол центрове в София, извършващи инвестиционни измами срещу чужденци. Затворени са и четири кол центъра във Варна, Бургас и София, използващи генерирани с ИИ крипто платформи; щети от 600 000 EUR при случая от октомври [S50][S51]
19 юни	Прокуратура на Република България	Заподозрян е използвал собствения мобилен телефон на жертвата, за да смени телефона и имейла за контакт в банковия ѝ профил, след което е кандидатствал за кредит от 25 000 EUR на нейно име през електронния канал на банката; щетата е за банката [S52]
14 август	Комисия за регулиране на съобщенията (КРС) и трите мобилни оператора	Съвместни действия срещу ръст на измамите с подправяне на номера на обаждащия се; регулаторът заяви, че подправянето не може да бъде спряно само с блокиране на номера [S63]
28 август	МВР	Фалшиви имейли с „призовка от полицията" използваха логата на полицията и Европол и имената на ръководители в полицията, за да обвинят получателите в престъпления [S53]
19 ноември	МВР	Дирекция „Киберпрестъпност" заяви, че получава над 100 сигнала на ден за отвлечени акаунти и приложения [S54]

Какво казва това на защитниците. Полицейските случаи, в които се посочват суми, описват измами с IBAN на получателя срещу фирми, инвестиционни кол центрове и, в един случай, кредит на името на жертва след смяна на данни за контакт. Те не описват продажбите на бази данни, които доминират в заглавията за тъмната мрежа. SMS вълните имитират институциите, на които гражданите най-вероятно ще се подчинят: полицията, транспортното министерство и куриерите. Контролите са процедурни и технически. Те включват потвърждение по независим канал при смяна на контакт или получател на плащания, допълнителни проверки за кредити след всяка промяна на профила, премахване на имитиращи домейни и предупреждения към клиентите при всяка вълна.

ОСНОВНИ ИЗВОДИ

01

Документите за самоличност и търговията с акаунти, а не кражбата на карти, са най-големите специфични за България сигнали за измами в нашите данни.

02

Данните за карти обхващат само карти, видени в явен текст в събраните публикации (§8.2).

03

Полицейските случаи сочат SMS фишинг от името на полицията и куриери, инвестиционни кол центрове и, в един случай, кредит след смяна на данните за контакт в банков профил.

ГЛАВА 9

Банки и финанси: задълбочен анализ

ТАЗИ ГЛАВА ОТГОВАРЯ НА ВЪПРОСА

Къде се намира видимата експозиция на българските банки: в самата банка, при служителите ѝ или при клиентите ѝ?

4 от 16

банки, издаващи карти, с актуална обява за идентификационни данни, първото за приоритизиране

НАКРАТКО

По-голямата част от видимата експозиция е при клиентите: 18 742 асоциации с устройства извън класификацията за служители при 16-те банки, издаващи карти, резултати от проверка на карти и търговия с български банкови сметки. Сигналите при банките и служителите са актуални обяви при 4 от 16 банки и 67 устройства на служители. Три банки носят две трети от сигнала за клиентски устройства. Първо обработете всяка актуална обява, после проверете устройствата на служителите. Следете отказите от проверки на карти във вашите BIN диапазони (BIN е префиксът на издателя в номера на картата).

Тази глава обхваща 16-те банки, издаващи карти, сред 31-те организации от банковия и финансовия сектор в глава 3. Останалите 15 са централната банка, банка за развитие, пазарна инфраструктура, платежни институции и дружества за електронни пари, фирми за потребителски кредити, пенсионни фондове и клон на чуждестранна банка. Затова 18 742 устройства извън класификацията за служители тук се различават от 34 765 там, а 67 устройства на служители от 126. По същата причина 4 от 12-те актуални обяви в сектора са при банки. Само обобщени данни; отделните банки не се назовават.

4 от 16

банки, издаващи карти, с актуална обява за идентификационни данни (4 от 12-те в сектора; останалите 8 са при организации, които не издават карти)

16 от 16

банки, издаващи карти, с асоциации с устройства извън класификацията за служители (общо 18 742; собствеността и актуалното заразяване са непотвърдени)

9 от 16

банки, издаващи карти, с устройства, класифицирани като на служители (общо 67)

12 от 16

банки, издаващи карти, които налагат DMARC (20 от 31 в сектора)

12 от 16

банки, издаващи карти, с карти в явен текст в събрани публикации (70 от 126-те карти посочват една от тях; тесен обхват, §8.2)

Трите банки с най-много асоциации с устройства извън класификацията за служители съставляват 66% от тях.

Какво означава това за банките.

1. **Актуалните обяви са на първо място.** 4 от 16 банки имаха такава в деня на проверката; приложете решение 1 (документирано решение в рамките на 5 работни дни).
2. **Експозицията на служителите е малка, но реална.** 67 устройства, класифицирани като на служители, при 9 банки са подмножеството, което има значение за проникване. След актуалните обяви те заслужават приоритетна проверка пред много по-голямата бройка извън класификацията за служители.
3. **Асоциациите с устройства извън класификацията за служители са по-голямата експозиция.** 18 742 асоциации с устройства при всичките 16 банки не са класифицирани като на служители и най-вероятно са устройства на клиенти. Собствеността, актуалното заразяване и дали някоя съхранена сесия или парола все още работи са непотвърдени и изискват проверка. Екипите за борба с измамите трябва да използват сигнали за риск от устройството и сесията при вход и при промяна на получатели на плащания, а не само проверки на паролата.

4. **Проверката на карти е откриваем предвестник.** Ботовете за проверка на карти ги тестват с малки авторизации или опити за добавяне на карта в шлюзовете на търговци. Издателите могат да откриват клъстери от отказани опити с малка стойност от чуждестранни шлюзове в своите BIN диапазони и да идентифицират засегнатите карти. След това могат да проверят сигналите за авторизация и измами по тях и да преиздадат картите с потвърден риск съгласно политиката на издателя.
5. **Сметките на „мулета“ и превземането на профили са рискът надолу по веригата.** Публикациите за търговия със сметки търсят български банкови сметки (§8.1). Един полицейски случай описва кредит, изтеглен след като данните за контакт на жертвата са били променени от собствения ѝ телефон (§8.5). Контролите при откриване на клиенти и при промяна на профила трябва да приемат, че ЕГН, датата на раждане и адресът са известни на престъпниците (§4.4).

ОСНОВНИ ИЗВОДИ

01

Първо са актуалните обяви за идентификационни данни при 4 от 16 банки, издаващи карти, после 67-те устройства на служители. Другите 18 742 устройства също се нуждаят от проверка.

02

12 от 16 банки, издаващи карти, налагат DMARC; четири не го правят.

03

Отказите от проверки на карти във вашите BIN диапазони и промените в данните за контакт на клиентите са откриваеми предвестници.

ГЛАВА 10

Регулаторна рамка и национален отговор

ТАЗИ ГЛАВА ОТГОВАРЯ НА ВЪПРОСА

Какво се промени в правилата за киберсигурност в България през 2026 и какво трябва да има организацията сега, след като периодът на намалени глоби приключи?

24 ч

за ранно предупреждение за значителен инцидент според изменения Закон за киберсигурност

НАКРАТКО

През 2026 правилата за киберсигурност в България бяха пренаписани. Измененията на Закона за киберсигурност транспонират NIS2, с ранно предупреждение до 24 часа и глоби до 10 милиона EUR или 2% от оборота. Намалението на глобите с 50% се прилагаше само за нарушения до 1 юни 2026. Ново министерство ръководи електронното управление и киберсигурността, а наказателната процедура на ЕС е прекратена. Потвърдете дали сте съществен или важен субект и тествайте още сега канала си за докладване в рамките на 24 часа.

Мярка	Какво успяхме да проверим	Статус и уговорки
Изменения на Закона за киберсигурност (NIS2)	Приети от Народното събрание на 5 февруари 2026, обнародвани с Указ № 52 от 11 февруари и публикувани в Държавен вестник, бр. 17 от 13 февруари 2026 [S28]	Публикуваният текст не посочва отделна дата на влизане в сила; редица срокове за прилагане текат от влизането в сила на закона; приемаме, че задълженията са в сила, затова потвърдете датата на влизане в сила с юрист
Обхват	Съществените субекти са основно видовете по Приложение I над прага за средно предприятие, плюс някои категории независимо от размера (напр. административни органи, доставчици на DNS и удостоверителни услуги); важните субекти са останалите видове по Приложения I и II (чл. 4а) [S28]	Субектите се идентифицират от компетентните органи след решение на Министерския съвет (§47-48) [S28]
Докладване на инциденти	Ранно предупреждение до 24 часа след откриване на значителен инцидент, уведомление до 72 часа и окончателен доклад не по-късно от един месец след уведомлението (чл. 23, ал. 5) [S28]	Прилага се за съществените и важните субекти. Доставчиците на удостоверителни услуги уведомяват до 24 часа; междинен доклад се подава по искане на CSIRT; ако инцидентът не е овладян до един месец, следва междинен доклад, а окончателен доклад до един месец след овладяването [S28]
Глоби: съществени субекти	Имуществена санкция за организацията до 10 000 000 EUR или 2% от общия годишен световен оборот, като се прилага по-високата сума, но не по-малко от 25 000 EUR (чл. 29, ал. 2) [S28]	Ал. 2 не се прилага за съществените субекти, които са административни органи (чл. 29, ал. 5). За нарушения до 1 юни 2026 санкциите бяха намалени с 50% (§51); този период е приключил [S28]
Глоби: важни субекти и ръководство	Важни субекти: имуществена санкция до 7 000 000 EUR или 1,4%, но поне 12 500 EUR (чл. 29, ал. 3). Лични глоби 500–5 000 EUR за ръководители, управители и членове на управителния орган при нарушения по чл. 21 (чл. 29, ал. 4) [S28]	Същото намаление с 50% се прилагаше до 1 юни 2026 [S28]
Регистър	Отговорният министър води регистър на обхванатите субекти; промените се съобщават в срок от две седмици (чл. 6) [S28]	Законът посочва министъра на електронното управление; през май това министерство беше слято с Министерството на иновациите и дигиталната трансформация [S26]; не успяхме да потвърдим кое министерство води регистъра сега

Мярка	Какво успяхме да проверим	Статус и уговорки
Подзаконови актове	В срок от 6 месеца от влизането в сила Министерският съвет определя компетентните органи и приема методиката за идентификация. Наредба следва в срок от 8 месеца, а нова национална стратегия в срок от 9 месеца (§47) [S28]	До датата на отсечката не успяхме да потвърдим, че всяка стъпка е изпълнена
Наказателна процедура на ЕС	Европейската комисия прекрати наказателната процедура 2024/0257 срещу България, след като на 6 март 2026 беше нотифицирано пълното транспониране, съобщи министерството на 1 октомври [S29]	Прекратена
Национална система за киберсигурност	На 4 ноември министерството съобщи за решение на Министерския съвет, с което се определят администрациите, включени в Националната система за киберсигурност [S60]	Списъкът на администрациите не беше публикуван в съобщението
DORA	Измененията в Закона за пазарите на криптоактиви правят БНБ компетентен орган за кредитните институции и, чрез Закона за платежните услуги и платежните системи, за платежните институции и дружествата за електронни пари; КФН отговаря за инвестиционните посредници, застрахователите, доставчиците на услуги за криптоактиви и други [S73]	DORA се прилага от 17 януари 2025; измененията са обнародвани в Държавен вестник, бр. 54 от 4 юли 2025 [S73]; по-ранен правен коментар [S58] описва законопроекта на етап внасяне; потвърдете компетентния си орган с юрист
Критични субекти (CER)	Проект на закон за устойчивостта на критичните субекти беше на обществено обсъждане от 27 май до 26 юни 2025 [S59]	Приемането не е потвърдено към датата на отсечката

Новата глава също така определя Съвета по киберсигурност за орган за управление при киберкризи (чл. 17а) и възлага на националния CSIRT ролята на координатор при координираното разкриване на уязвимости (чл. 19, ал. 4) [S28].

Прилага ли се измененият закон за вас? Таблицата тълкува структурата на закона [S28] за четири чести случая; потвърдете с юрист.

Организация	Вероятен режим	Действие сега
Банка, платежна институция, застраховател или инвестиционен посредник	DORA е секторният режим на ЕС за ИКТ риска и докладването на инциденти при финансовите субекти; проверете с юрист как българският закон урежда припокриването	Свържете докладването на големи инциденти по DORA с компетентния си орган (БНБ или КФН) и потвърдете с юрист дали е нужно паралелно уведомление до CERT България; тествайте го
Енергийна, транспортна, здравна, ВиК, цифрова инфраструктура или друга организация по Приложение I над средния размер	Съществен субект	Регистрирайте се; определете лицето, което изпраща ранното предупреждение до 24 часа; документирайте одобрението на мерките за сигурност от ръководството
Друга организация по Приложение I или II с поне среден размер, включително производители, пощенски и куриерски услуги, храни и химикали	Обикновено важен субект; някои видове са обхванати или съществени независимо от размера (чл. 4 и 4а), затова потвърдете с юрист	Същото задължение за докладване; по-нисък максимален размер на глобата
Държавна или общинска администрация	Обхваната от закона и, когато е определена, от Националната система за киберсигурност [S60]	Потвърдете включването в националната система; съгласувайте журналирането с нея

Какво да направят CISO сега. Потвърдете писмено дали сте съществен или важен субект и се регистрирайте в министерството, което води регистъра (уточнете кое с юрист). Определете лицето, което изпраща ранното предупреждение, и му осигурете канал за 24 часа, който работи и през почивните дни. Проведете упражнение по уведомлението до 72 часа и окончателния доклад в едномесечния срок с реален минал инцидент, включително междинния доклад при неовладян инцидент. Поддържайте датиран запис за одобрението на

мерките за сигурност от ръководството, защото членовете на управителния орган вече могат да бъдат глобени за нарушения на задълженията за мерки за сигурност. Този раздел не е правен съвет.

ОСНОВНИ ИЗВОДИ

01

Измененията по NIS2 бяха обнародвани на 13 февруари 2026, с ранно предупреждение до 24 часа и глоби до 10 милиона EUR или 2% от оборота.

02

Намалението на глобите с 50% се прилагаше само за нарушения до 1 юни 2026.

03

Регистрирайте се, определете отговорника за докладване на инциденти и тествайте канала за 24 часа още сега.

ГЛАВА 11

Перспективи

ТАЗИ ГЛАВА ОТГОВАРЯ НА ВЪПРОСА

За какво трябва да се подготвят българските организации и какви данни биха променили този план?

5
ключови оценки, всяка със сигнал за наблюдение

В ТАЗИ ГЛАВА

11.1 Ключови оценки | 11.2 Какво би променило оценката | 11.3 Условни сценарии

НАКРАТКО

Планирайте за същите видове данни, а не за нова заплаха. Това са излагане на самоличности, което остава невидимо до използването му, и обяви на рансъмуер групи в брой като в Румъния и Гърция. Към тях се добавят дълготраен шпионски достъп до системи за документооборот и поща и повтарящи се измами от името на официални институции. Нямаме съпоставим времеви ред, за да кажем дали някоя от тях нараства. Променяйте плана, когато се променят данните по-долу, а не по календар.

11.1 Ключови оценки

Оценка	Степен на увереност	Основание и ограничение
Излагането на самоличности (устройства, stealer логове, обяви за идентификационни данни) е най-разпространеният измерим риск за водещите организации в България	Висока за списъка от 250 организации	Броят в глава 3; не е национално разпространение; сигнал: нови актуални обяви или връзки с устройства на служители за вашите домейни
Рансъмуер групите обявяват български организации в брой, сравним с Румъния и Гърция	Висока за наблюдаваните обяви	19 обяви през 2026 срещу 20 и 19; непубликуваните инциденти са невидими; сигнал: обяви в Ransompedia или оповестен инцидент в българска организация
Ако системите за документооборот и поща нямат централно журналиране, планирайте за дълготраен шпионски достъп	Средна (допускане за планиране)	Едно официално съобщено многогодишно проникване; входният път не е публичен; сигнал: нови официални разкрития или доклади на доставчици
Планирайте за нови предложения на български данни за самоличност, включително ЕГН	Средна (допускане за планиране)	Предложения на застрахователни данни и потвърдени уведомления за нарушения от три застрахователни дружества от две групи през 2026; автентичността на предложенията не е проверена; сигнал: нови предложения в наблюдаваните канали
Планирайте за повтарящи се вълни от измами от името на полицията, транспортното министерство и куриерите, както и за примамки, свързани с обществени промени като преминаването към еврото	Средна (допускане за планиране)	Повтарящи се официални предупреждения през май, август и ноември; сигнал: нови домейни имитатори и предупреждения на CERT

11.2 Какво би променило оценката

Текущо тълкуване	Данни, които биха го променили	Засегнато решение
Обявите на рансъмуер групите са твърдения	Разкрит рансъмуер инцидент при български съществен субект	Повишете готовността за рансъмуер; първо проведете теста за възстановяване от §12.1

Текущо тълкуване	Данни, които биха го променили	Засегнато решение
Предложенията на застрахователни данни не са проверени	Извадка, съпоставена със схемата на конкретна система; записи, потвърдени от администратора на данните; или констатация на регулатор	Съвпадението със схема задейства разследване и оценка от гледна точка на защитата на данните и правото; потвърдените записи или констатация на регулатор задействат решението за уведомяване и защитата на клиентите
Проникването в държавните мрежи не е приписано на конкретен извършител	Официално приписване или такова от доставчик, с индикатори	Заредете индикаторите; търсете следи в системите за документооборот и поща
Текущите обяви означават „проверете“, а не „пробив“	Проверката показва активни акаунти без MFA сред обявените идентификационни данни	Ескалирайте към реагиране при инциденти и наложете MFA за засегнатите потребители
Хактивистките твърдения срещу България са малко	Продължителна DDoS кампания срещу портали за граждани, потвърдена от засегнатата организация	Преразгледайте капацитета за защита на ниво доставчик и плановете за непрекъснатост на услугите

11.3 Условни сценарии

- **Ако** бъде обявено национално събитие, кампания за глоби или промяна в плащанията, **тогава** планирайте за фишинг по SMS и имейл от името на съответната институция (допускане за планиране). **Сигнал:** нови домейни имитатори и предупреждения на CERT. **Решение:** публикувайте предупреждение към клиентите и поискайте премахване на домейните.
- **Ако** бъде разкрита нова критична уязвимост в изложен към интернет продукт за поща, VPN или защитна стена, **тогава** планирайте за опити за експлоатация срещу държавни, енергийни и телекомуникационни организации. **Сигнал:** бюлетини на CERT България и на доставчиците. **Решение:** инсталирайте корекцията и проверете системите, изложени към интернет, в рамките на вашия срок, след това търсете web shell скриптове и нови администраторски акаунти.
- **Ако** активността на checker ботове по вашите BIN диапазони нарасне и разследването потвърди, че конкретни карти се тестват, **тогава** планирайте за опити за измами без физическо присъствие на картата с тези карти. **Сигнал:** групирани откази на малки суми от чуждестранни платежни шлюзове. **Решение:** разследвайте опитите, проверете сигналите за оторизация и измами и преиздайте картите с потвърден риск.

ОСНОВНИ ИЗВОДИ

01

Планирайте за видове данни, а не за нова заплаха: излагане на самоличности, обяви за изнудване, дълготраен шпионски достъп и повтарящи се измами от името на официални институции.

02

Всяка оценка има сигнал; променяйте плана, когато сигналът се промени.

03

Все още няма съпоставим времеви ред, който да покаже дали някоя от тези заплахи нараства.

ГЛАВА 12

План за действие

ТАЗИ ГЛАВА ОТГОВАРЯ НА ВЪПРОСА

Какво трябва да направи всеки екип през следващите 90 дни и как съветът на директорите ще знае, че е изпълнено?

20
действия с отговорник и доказателство за изпълнение

В ТАЗИ ГЛАВА

12.1 30/60/90 дни | 12.2 По роли | 12.3 Как може да помогне Brandefense

НАКРАТКО

Първо потвърдете, че получавате сигнали за обяви и устройства. После действайте по данните, които засягат конкретно вас: текущи обяви за идентификационни данни и връзки с устройства на служители. Обновете изложените към интернет пощенски и периферни системи като базова хигиена. След това затворете пропуските в докладването, фишинга, промените в плащанията и удостоверяването на пощата и проведете упражнение с рансъмуер обява и твърдение за данни за самоличност. Съветът на директорите вижда изпълнението от доказателството за всеки ред и от таблицата с показатели по-долу; докладвайте и двете до ден 90.

12.1 30/60/90 дни

Това е последователност, а не период на изчакване. Текуща съществена заплаха трябва да влезе незабавно във вашия процес за инциденти.

1 Дни 1-30

Потвърдете, че получавате сигнали за обяви за идентификационни данни и за заразени устройства за основните си домейни. Ако не, осигурете ги и отбележете редовете за проверка на обявите и устройствата на служители като блокирани до пристигането на сигналите

ОТГОВОРНИК
CISO и разузнаване на заплахи

ДОКАЗАТЕЛСТВО ЗА ИЗПЪЛНЕНИЕ
Посочен източник на сигнали; получен първи сигнал

За всяка текуща обява за идентификационни данни, свързана с вашите домейни, проверете акаунта и състоянието на MFA в срок от 5 работни дни

ОТГОВОРНИК
Екип по идентичности

ДОКАЗАТЕЛСТВО ЗА ИЗПЪЛНЕНИЕ
Всяка обява има решение с дата: нулиране, вече отстранено или не е наша

2 Дни 31-60

Включете централно журналиране за системите за документооборот, поща и идентичности и пазете записите достатъчно дълго, за да можете да погледнете месеци назад, а не дни (§7.2)

ОТГОВОРНИК
SOC и инфраструктура

ДОКАЗАТЕЛСТВО ЗА ИЗПЪЛНЕНИЕ
Записани източници на журнали и срок на съхранение; проведено едно ретроспективно търсене

Където DMARC е p=none, липсва или е невалиден, инвентаризирайте изпращачите и въведете налагането поетапно

ОТГОВОРНИК
Екип по пощата

ДОКАЗАТЕЛСТВО ЗА ИЗПЪЛНЕНИЕ
Съгласувани изпращачи; p=quarantine с път за връщане назад

3 Дни 61-90

Извадете от интернет интерфейсите за управление на камери, контролери и операторски панели; премахнете паролите по подразбиране

ОТГОВОРНИК
OT и поддръжка на сгради

ДОКАЗАТЕЛСТВО ЗА ИЗПЪЛНЕНИЕ
Външното сканиране не показва изложени интерфейси за управление

Подпишете DNS за основните домейни, където регистраторът ви поддържа това; поправете невалидните TLS сертификати и добавете HSTS

ОТГОВОРНИК
Мрежови и уеб екипи

ДОКАЗАТЕЛСТВО ЗА ИЗПЪЛНЕНИЕ
Валидирането на DNSSEC от външен резолвер е успешно; проверките на сертификатите са успешни

Проверете връзките с устройства, класифицирани като на служители; отменете сесиите и токените, където са активни

ОТГОВОРНИК
Екипи по идентичности и крайни точки
ДОКАЗАТЕЛСТВО ЗА ИЗПЪЛНЕНИЕ
Списъкът с устройства е съгласуван с инвентара на активите; отменените са записани

Базова хигиена (§11.3): потвърдете, че всеки изложен към интернет пощенски, VPN, защитен или периферен сървър е обновен до текущата коригирана версия на доставчика, и търсете web shell скриптове и нови администраторски акаунти

ОТГОВОРНИК
Инфраструктура
ДОКАЗАТЕЛСТВО ЗА ИЗПЪЛНЕНИЕ
Външният повторен тест е успешен; търсенето е приключено

Потвърдете дали сте съществен или важен субект, регистрирайте се в министерството, което води регистъра (уточнете кое с юрист, §10), и определете лицето, което изпраща ранното предупреждение до 24 часа

ОТГОВОРНИК
CISO и правен отдел
ДОКАЗАТЕЛСТВО ЗА ИЗПЪЛНЕНИЕ
Писмено становище; подадена регистрация или датата и причината, ако тя още предстои; определен отговорник; тестван канал за контакт

Определете говорителя и канала за изявления за състоянието на услугите при DDoS и за непроверени твърдения за изтичане

ОТГОВОРНИК
Комуникации и CISO
ДОКАЗАТЕЛСТВО ЗА ИЗПЪЛНЕНИЕ
Одобрен наръчник от една страница

Преминете към устойчиво на фишинг MFA (ключове за сигурност FIDO2, passkeys или вход със сертификат) за администраторите на пощата, привилегированите и отдалечените потребители

ОТГОВОРНИК
Екип по идентичности
ДОКАЗАТЕЛСТВО ЗА ИЗПЪЛНЕНИЕ
Обхватът е записан по групи потребители

Задайте сигнали при масово създаване на пощенски кутии и при вход в администрацията на пощата от нови местоположения, чрез журнала за администраторски одит на пощенската платформа и журнала за вход на доставчика на идентичност (Случай C)

ОТГОВОРНИК
SOC
ДОКАЗАТЕЛСТВО ЗА ИЗПЪЛНЕНИЕ
Сигналът е активен и тестван

Тествайте процесите за възстановяване на акаунт, промяна на данни за контакт и промяна на получател срещу нападател, който знае ЕГН, дата на раждане и адрес; добавете допълнителни проверки преди кредити след промяна на профила (§8.5)

ОТГОВОРНИК
Екипи по измамите и клиентските операции
ДОКАЗАТЕЛСТВО ЗА ИЗПЪЛНЕНИЕ
Слабостите са записани и отстранени; повторният тест е успешен

Изисквайте потвърждение по независим канал за промени в платежни нареждания и получатели

ОТГОВОРНИК
Финанси и екип по измамите
ДОКАЗАТЕЛСТВО ЗА ИЗПЪЛНЕНИЕ
Процедурата е одобрена; една симулирана заявка е засечена

Публикувайте предупреждения към клиентите, съобразени с всяка вълна от SMS фишинг от името на полицията, транспортното министерство или куриерите, и поискайте премахване на домейните имитатори

ОТГОВОРНИК
Екип по измамите и комуникации
ДОКАЗАТЕЛСТВО ЗА ИЗПЪЛНЕНИЕ
Предупрежденията са издадени; заявките за премахване са записани

Проведете настолно упражнение, което съчетава обява на сайт за изтичане на рансъмуер група с едновременно твърдение за клиентски данни

ОТГОВОРНИК
CISO, комуникации, правен отдел
ДОКАЗАТЕЛСТВО ЗА ИЗПЪЛНЕНИЕ
Дневник на решенията и времената, включително ранното предупреждение до 24 часа

Докладвайте таблицата с показатели спрямо целите (по-долу)

ОТГОВОРНИК
CISO към съвета на директорите
ДОКАЗАТЕЛСТВО ЗА ИЗПЪЛНЕНИЕ
Документ за съвета с оставащите пропуски и отговорниците

Задайте сигнали при групирани откази от checker ботове по вашите BIN диапазони

ОТГОВОРНИК
Екип по измамите

ДОКАЗАТЕЛСТВО ЗА ИЗПЪЛНЕНИЕ
Сигналът е активен; първият преглед е записан

Проведете тест за възстановяване с измерване на времето за една ключова система

ОТГОВОРНИК
Инфраструктура

ДОКАЗАТЕЛСТВО ЗА ИЗПЪЛНЕНИЕ
Времето за възстановяване е записано спрямо целевото време за възстановяване (RTO: най-дългото прекъсване, което планът ви за непрекъснатост допуска)

Договорете или тествайте защита от DDoS на ниво доставчик за порталите за граждани и клиенти преди следващото национално събитие

ОТГОВОРНИК
Инфраструктура и снабдяване

ДОКАЗАТЕЛСТВО ЗА ИЗПЪЛНЕНИЕ
Протокол от теста на защитата

Целеви стойности на показателите. Това са препоръчителни стойности по подразбиране; задайте свои, където политиката ви е различна.

Показател	Цел
Наблюдение на обяви за идентификационни данни и заразени устройства за основните домейни, вътрешно или чрез доставчик	Въведено до ден 30
Текущи обяви с решение в срок от 5 работни дни	100% до ден 90
Устройства, класифицирани като на служители, съгласувани с инвентара на активите	100% до ден 90
Изложени към интернет пощенски и периферни сървъри, преминали външен повторен тест	100% до ден 90
Определен статус по NIS2 и определен отговорник за докладване на инциденти	До ден 30
Тестван 24-часов канал за ранно предупреждение, включително през уикенд	До ден 30
Централизирани журнали за документооборот, поща и идентичности със срок за ретроспективен преглед	До ден 60
Основни домейни с DMARC на quarantine или reject	100% или датиран план до ден 90
Администратори на пощата, привилегировани и отдалечени потребители с устойчиво на фишинг MFA	100% или датиран план до ден 90
Промени на получатели и данни за контакт, потвърдени по независим канал	100% до ден 90
Тест за възстановяване в рамките на RTO	Успешен или с датирано решение до ден 90

12.2 По роли

Роля	Първо решение
Съвет на директорите	Поискайте броя на текущите обяви и устройствата на служители за вашата организация, датата, до която всяко ще бъде проверено, и становището за статуса по NIS2
CISO	Първо въведете наблюдението на обяви и устройства, след това проверете актуалните обяви и устройствата на служителите, после въведете централното журналиране; обновявайте периферните системи паралелно като базова хигиена
SOC	Добавете детекции за web shell скриптове на пощенски и периферни сървъри (журнали на уеб сървъра и EDR), нови администраторски акаунти (журнал на директорията), масово създаване на пощенски кутии (одитен журнал на пощата) и вход в администрацията от нови места (журнал за вход)
Екип по измамите	Приемайте, че ЕГН, датата на раждане и адресът са известни; добавете допълнителни проверки след промени в профила; наблюдавайте групираните откази от checker ботове по вашите BIN
Комуникации	Подгответе изявления за DDoS, рансъмуер обяви и непроверени твърдения за изтичане, които разграничават твърдение, проверен факт и действие

ОСНОВНИ ИЗВОДИ

01

Потвърдете наблюдението, след това проверете текущите обяви и устройствата на служители и изяснете статуса си по NIS2 през първите 30 дни.

02

До ден 60 включете централно журналиране, устойчиво на фишинг MFA за администраторите на пощата и проверки по независим канал за промени в плащанията и контактите.

03

Проведете упражнение с комбиниран сценарий на рансъмуер обява и твърдение за данни и докладвайте таблицата с показатели до ден 90.

12.3 Как може да помогне Brandefense

Brandefense съчетава разузнаване на киберзаплахи (Cyber Threat Intelligence), защита от цифрови рискове (Digital Risk Protection) и управление на външната повърхност за атака (External Attack Surface Management). Анализът в този доклад използва същите данни, които платформата прилага към наблюдаваните организации. Това са връзки със заразени устройства и идентификационни данни, текущи обяви на пазари за идентификационни данни, домейни имитатори, изложени документи и споменавания в тъмната мрежа. Анализът не обещава, че всяко твърдение може да бъде проверено или че исторически запис остава използваем.

Донесете своите домейни, марки и приоритети по сигурността на 30-45-минутна демонстрация с екипите по продажби и предпродажбена подкрепа. Екипът може да покаже как наблюдението в платформата свързва външните сигнали с активите, които управлявате. Член на екипа на Brandefense или партньор във вашия регион ще се свърже с вас.

Заявете демонстрация

Приложение A. Метод

A.1 Период, източници и приоритет

Периодът на изследването е 1 януари-18 ноември 2026 по датата на публикуване на публикацията. На първо място са собствените данни. Това са Brandefense Blackhole (публикации в тъмната мрежа и в приложения за съобщения, връзки със заразени устройства и идентификационни данни, данни за карти), Ransompedia (обяви на рансъмуер групи) и оценките на излагането от Brandefense Atlas. Външните източници дават контекст и се цитират само след прочит на подкрепящия пасаж. Данните са извлечени на 21 ноември 2026.

Източниците S1, S3-S6 и S8 са собствени данни на Brandefense и нямат публичен адрес. Пропуските в номерацията на източниците са умишлени, а всеки външен източник в Приложение C има връзка и дата на отваряне.

A.2 Публикации в Blackhole

Елемент	Стойност
Публикации, маркирани като отнасящи се до България	14 289
Свързани публикации	9 862
Маркирани публикации след преглед	7 148–7 529
Публикации, специфични за България	1 757 в етикетирания набор; 3 325 в обединения корпус

Бройките след преглед все още включват част от рекламите за няколко държави. Затова отчитаме и набора, специфичен за България, в който България е предметът на публикацията. И двата набора остават горни граници за престъпната дейност, свързана с България.

Публикациите с етикет за български език рязко намаляват от юни, а месечните редове не са сравними преди и след средата на 2026 г. Затова не сравняваме категории или езици през годината и не тълкуваме промените от юни нататък като тенденции.

A.3 250-те организации

Подборът, проверката и ограниченията са описани в §3.1. За всеки основен домейн отчитаме следните сигнали за излагане: заразени устройства, устройства на служители, записи с идентификационни данни, споменавания в тъмни чатове и в тъмната мрежа и нови домейни имитатори. Към тях се добавят документи, които споменават домейна, и текущи и минали обяви на пазари за идентификационни данни. Данните са прочетени на 21 ноември 2026.

A.4 Оценки на Atlas

Всяка организация получи оценка на излагането от Atlas от 0 (не е наблюдаван риск) до 100. Този доклад публикува само националната обобщаваща оценка за 250-те организации: 50 от 100. Приемайте актуалната обява за идентификационни данни като повод за проверка на акаунтите, а не като доказателство за пробив.

A.5 Проверки на DNS, TLS и уебсайтове

Резултатите обхващат записите за поща, SPF, DMARC, DKIM, DNSSEC и CAA (разрешение за удостоверяващ орган), TLS и началната страница на всеки домейн. Липсващите, невалидните и само наблюдаващите (p=none) политики DMARC се отчитат като липса на налагане.

Индексът на пасивната хигиена е аналитичен композитен показател на Odin от тези проверки на имейл, DNS, TLS и заглавки, по скала 0–100. По-висока стойност означава по-слаба хигиена; това е модел, а не оценка на Atlas.

A.6 Данни за карти в публикации

Обхват: само платежни карти, които се появяват в явен текст в публикациите от тъмната мрежа, събрани за този доклад. Brandefense открива откраднати карти и чрез много други методи, които са извън този доклад. Тези данни не измерват кражбата на карти или загубите от измами.

A.7 Рансъмуер

Използвахме обявите от Ransompedia за България, Румъния, Гърция, Сърбия и Северна Македония след преглед, за всички дати, датирани по публикуване. Публичен тракер и препредадени публикации от Blackhole се използват само за кръстосана проверка.

A.8 Обхват на инцидентите

Проверихме всяка от 250-те организации в нашите данни за 1 януари-18 ноември 2026. Прочетохме и страниците с официални новини и предупреждения месец по месец за януари-ноември 2026. Сред тях са тези на националния CERT, министерството на електронното управление, МВР, Прокуратурата, КФН и КЗЛД. Търсихме публични материали на английски, български, руски и турски до 21 ноември 2026.

Проверка за пропуски (21 ноември 2026). Независима проверка за пропуски добави два елемента: инцидент, оповестен от хостинг доставчик (§7.6), и доклад на доставчик за отвлечен сайт от военния сектор (§7.2). Добавихме също официална оценка на измамите с IBAN на получателя и предупреждение за подправяне на номера на обаждащия се. Добавихме и доклад на изследователи за пощенските кутии на местни служители, както и подробности за юлската вълна от заплахи за бомби. Някои твърдения с правителствена тематика не можаха да бъдат потвърдени и не са използвани.

Оставащи ограничения на обхвата. Нашата картина е частична:

- Някои официални сайтове не можаха да бъдат прочетени. Сайтовете на ДАНС, Централната избирателна комисия и Националната агенция за приходите не можаха да бъдат прочетени; намерихме изявленията им от 2026 г. само чрез медийни публикации.
- Търсачките индексират малка част от архива на националната информационна агенция за 2026 г., затова обхватът му месец по месец остава непълен.
- Сайтовете за изтичане на рансъмуер групи в Tor са обхванати само чрез Ransompedia.
- Затворените форуми и форумите само с покана, частните Telegram групи и продажбите, уговорени в лични съобщения, са извън нашето събиране.
- Публикациите, изтрити преди събирането, липсват.
- Инцидентите, които организациите обработват без разкриване, остават невидими.

Това, че даден инцидент липсва в този доклад, не означава, че не се е случил.

A.9 Степен на увереност и граници

Високата степен на увереност се отнася до възпроизводимо измерване, а не до самото твърдение на престъпника. Средната означава тълкуване с ясна подкрепяща линия и посочени ограничения. „Непроверено" означава, че не е установено независимо; това не е доказателство нито за измислица, нито за пробив. Организациите жертви се описват чрез ролята си; държавен орган се назовава само когато официално изявление потвърждава инцидента. Псевдонимите на извършителите се отпечатват; връзки, контакти, индикатори и лични данни се пропускат. Пълният произход на данните се съхранява във вътрешен регистър на доказателствата.

Приложение B. Регистър на доказателствата

Избрани публикации са възпроизведени като редактирани карти на публикации в посочената глава. Откъсите са кратки; пропуските са отбелязани с [...]; идентификаторите, контактите, връзките и организациите жертви са заменени с етикети в квадратни скоби съгласно правилата в A.9. Преводите са наши. Датите на публикуване не са дати на проникване. Идентификаторите на публикациите, връзките и пълният текст се съхраняват във вътрешен регистър на доказателствата.

Карта	Публикувана	Място	Псевдоним, както е показан	Език	Показана в
B01	2026-08-30	Telegram канал за търговия с лийдове	Lead-trading channel	английски	§4.4
B02	2026-09-10	Форум за киберпрестъпност	lauraallen	английски, извадка на български	§4.4
B03	2026-08-11	Канал за хакерски новини, препредаващ тема от форум	Relay channel	английски	§4.5
B04	2026-04-05	Форум за киберпрестъпност	DuperKinger123	английски	§4.5

Карта	Публикувана	Място	Псевдоним, както е показан	Език	Показана в
B05	2026-04-20	Форум за киберпрестъпност	thejackal101	английски	§4.6
B06	2026-08-08	Форум за киберпрестъпност	kookiegst	английски	§4.6
B07	2026-02-16	Форум за кракване	UHQCombos	английски	§4.6
B08	2026-02-18	Форум за пробиви	Jurak	английски	§4.6
B09	2026-02-23	Форум за пробиви	Commando	английски	§4.6
B10	2026-03-05	Канал с onion връзки, препредаващ твърдение	TheGarudaEye (relayed)	английски	§6.2
B11	2026-10-14	Испаноезичен канал за препредаване	Z-Alliance / Z-Pentest (relayed)	испански	§6.4
B12	2026-08-22	Форум за изтичания	Enigma Group	английски	§4.5
B13	2026-04-29	Telegram чат на хакерски форум	wat4ri	английски	§4.6
B14	2026-07-12	Telegram чат за регистрации и работа	mansorryuwu	английски	§8.1
B15	2026-11-05	Форум за кракване	annabelle0	английски	§8.3
B16	2026-08-23	Форум за изтичания	updap (forum poster)	английски	§4.6
B17	2026-01-29	Форум за пробиви	temporary	английски, извадка на български	§4.6
B18	2026-07	Бот за наблюдение на изтичания, препредаващ тракер	Leak-monitor bot	английски	§7.4

Приложение C. Източници

S1 Публикации в Brandefense Blackhole, отнасящи се до България, дати на публикациите 1 януари–18 ноември 2026, извлечен на 21 ноември 2026.

S3 Връзки на Brandefense Blackhole със заразени устройства, бази данни от пробиви, stealer логове и combolist списъци за 250 домейна, прочетени на 21 ноември 2026.

S4 Оценки на излагането и сигнали от Brandefense Atlas за 250-те домейна, 21 ноември 2026, включително обяви на пазари за идентификационни данни, домейни имитатори, изложени документи и статистика на споменаванията.

S5 Публични проверки на DNS, TLS и началната страница на 250-те домейна от Brandefense, 21 ноември 2026.

S6 Brandefense Ransompedia, обяви след преглед за България, Румъния, Гърция, Сърбия и Северна Македония, всички дати, извлечени на 21 ноември 2026.

S7 ransomware.live, публичен тракер за рансъмуер (страницата за държавата не се посочва), достъпено на 21 ноември 2026 (само за кръстосана проверка). https://www.ransomware.live/ (URL на страницата не се посочва). Проверено на 21 ноември 2026.

S8 Brandefense Blackhole, карти, свързани с България, в събраните публикации (само бройки), 21 ноември 2026.

S14 DataReportal (Kepios), *Digital 2027: Bulgaria*, 5 ноември 2026 (данни за октомври 2026). https://datareportal.com/reports/digital-2027-bulgaria. Проверено на 21 ноември 2026.

S15 Европейска централна банка, прессъобщение за въвеждането в обращение на еврото в България, 1 януари 2026. https://www.ecb.europa.eu/press/pr/date/2026/html/ecb.pr260101~c830245e42.en.html. Проверено на 21 ноември 2026.

S16 Европейска комисия, Access2Markets, "Bulgaria adopts euro on 1 January 2026", 28 януари 2026. https://trade.ec.europa.eu/access-to-markets/en/news/bulgaria-adopts-euro-1-january-2026. Проверено на 21 ноември 2026.

S17 BNT, "Police issue fraud warning ahead of euro changeover in Bulgaria", 29 декември 2025, по информация на МВР. https://bntnews.bg/news/police-issue-fraud-warning-ahead-of-euro-changeover-in-bulgaria-1371604news.html. Проверено на 21 ноември 2026.

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

S19 News.bg, "След кибератака МС и МЕУ останаха без интернет" (След кибератака Министерският съвет и министерството на електронното управление останаха без интернет), 19 април 2026, по Nova. https://news.bg/politics/sled-kiberataka-ms-i-meu-ostanaha-bez-internet.html. Проверено на 21 ноември 2026.

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

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

S22 Министерство на иновациите и дигиталната трансформация, изявление от 5 август 2026 относно неразрешен достъп до административни мрежи. https://midt.gov.bg/bg/news/1351; материал на английски от BTA, 5 август 2026: https://www.bta.bg/en/news/bulgaria/1180195-government-uncovers-apparent-years-long-breach-of-administrative-networks. Проверено на 21 ноември 2026.

S23 Министерство на иновациите и дигиталната трансформация, изявление от 18 ноември 2026 относно операцията за кибершпионаж срещу държавната администрация. https://midt.gov.bg/bg/news/1614. Проверено на 21 ноември 2026.

S24 Mediapool, материал за брифинга на министъра относно петгодишното проникване, 18 ноември 2026. https://www.mediapool.bg/biznes/hakeri-imali-5-godini-dostap-do-darzhavni-mrezhi-iztochili-pone-62-mln-stranitsi-ot-dokumenti/. Проверено на 21 ноември 2026.

S25 Reuters, "Bulgaria uncovers five-year cyberespionage operation", 18 ноември 2026, препечатано от Internazionale. https://www.internazionale.it/ultime-notizie-reuters/2026/11/18/bulgaria-uncovers-five-year-cyberespionage-operation. Проверено на 21 ноември 2026.

S26 Решение на Народното събрание от 8 май 2026 за създаване на Министерство на иновациите и дигиталната трансформация, Държавен вестник, бр. 43 от 12 май 2026, по индекса на LexAlert. https://lexalert.bg/archive/2026/43/2543/; профил на министерството: https://midt.gov.bg/bg/about/ministry. Проверено на 21 ноември 2026.

S27 CERT България, национален екип за реагиране при инциденти с компютърната сигурност. https://www.govcert.bg/en/. Проверено на 21 ноември 2026.

S28 Закон за изменение и допълнение на Закона за киберсигурност, приет на 5 февруари 2026, Държавен вестник, бр. 17 от 13 февруари 2026 (официален текст). https://dv.parliament.bg/DVWeb/showMaterialDV.jsp?idMat=241234. Проверено на 21 ноември 2026.

S29 Министерство на иновациите и дигиталната трансформация, "Европейската комисия прекрати наказателна процедура № 2024/0257 срещу България", 1 октомври 2026. https://midt.gov.bg/bg/news/1561. Проверено на 21 ноември 2026.

S30 BNT, "Cyberattacks on Bulgaria on the rise", 16 март 2026, с думи на мениджъра по киберсигурност на Information Services. https://bntnews.bg/news/cyberattacks-on-bulgaria-on-the-rise-1383934news.html. Проверено на 21 ноември 2026.

S31 Държавна агенция "Национална сигурност", доклад за дейността през 2025, от 21 април 2026, публикуван от Министерския съвет. https://www.gov.bg/files/common/DANS%202025.docx. Проверено на 21 ноември 2026.

S32 DiarioBitcoin, материал за предложение във форум на 3,1 милиона записа, приписани на застраховател (заглавието назовава компанията), 10 септември 2026. https://www.diariobitcoin.com/ (адресът на статията е пропуснат). Проверено на 21 ноември 2026.

S34 e-security.bg, материал за потвърждението от КЗЛД на уведомления за нарушения от три застрахователни дружества от две групи (заглавието назовава компаниите), 26 септември 2026, по BIRD.BG. https://e-security.bg/ (адресът на статията е пропуснат). Проверено на 21 ноември 2026.

S35 CERT България, предупреждение за имейли със заплахи за бомби, изпратени до държавни институции от отвлечени акаунти, 9 юли 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/. Проверено на 21 ноември 2026.

S37 CERT България, предупреждение за атаки срещу изложени към интернет контролери за търговско хладилно оборудване, 6 ноември 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/. Проверено на 21 ноември 2026.

S38 МВР, изявление на министъра относно киберпрестъпността и дирекция "Киберпрестъпност", 20 юли 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. Проверено на 21 ноември 2026.

S39 МВР, задържане на двама заподозрени, свързани със "Smishing Triad", 18 март 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. Проверено на 21 ноември 2026.

S40 МВР, предупреждение за измами срещу продавачи в сайтове за обяви, 23 януари 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. Проверено на 21 ноември 2026.

S41 МВР, "Десетки хиляди фишинг съобщения са изпратени до потребители от името на институции и куриерски фирми", 11 май 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. Проверено на 21 ноември 2026.

S42 Прокуратура на Република България, Софийска градска прокуратура привлече обвиняем за компютърни престъпления, 30 октомври 2026. https://prb.bg/bg/news/80130-sofiyska-gradska-prokuratura-privleche-obvinyaem-za-kompyutarni-prestapleniya. Проверено на 21 ноември 2026.

S43 МВР, участие в операция Endgame, 13 ноември 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. Проверено на 21 ноември 2026.

S44 МВР, изземване от полицията в Пловдив на компютър със сканирани лични карти, 2 април 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. Проверено на 21 ноември 2026.

S45 КФН, предупреждение за фалшиви имейли от нейно име, 7 януари 2026. https://www.fsc.bg/falshivi-imejli-mamyat-ot-imeto-na-kfn/. Проверено на 21 ноември 2026.

S46 КФН, предупреждение за кражби на дружества за криптоактиви чрез подправени вписвания в регистъра, 3 февруари 2026. https://www.fsc.bg/kfn-preduprezhdava-za-krazhbi-na-kriptokompanii/. Проверено на 21 ноември 2026.

S47 МВР, предупреждение за SMS съобщения и съобщения в приложения за глоби за превишена скорост, 8 май 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. Проверено на 21 ноември 2026.

S48 CERT България, предупреждение за продължаваща SMS фишинг кампания, представяща се за полицията, пътната полиция и транспортното министерство, 18 май 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/. Проверено на 21 ноември 2026.

S49 CERT България, предупреждение за SMS фишинг относно електронни фишове, 11 ноември 2026. https://www.govcert.bg/warnings/phishing-november-2026/. Проверено на 21 ноември 2026.

S50 МВР, закриване на кол център в София за инвестиционни измами, публикувано на 10 юни 2026; текстът датира акцията на 4 юли 2026, затова датата на акцията остава неясна. 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. Проверено на 21 ноември 2026.

S51 МВР, закриване на четири кол центъра за измами с криптоинвестиции, генерирани с изкуствен интелект, 21 октомври 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. Проверено на 21 ноември 2026.

S52 Прокуратура на Република България, задържане за компютърна измама с променен банков профил и онлайн кредит, 19 юни 2026. https://prb.bg/bg/news/78652-po-iskane-na-sofiyska-rayonna-prokuratura-sadat-zadarzha-mazh-za-kompyutarna-izm. Проверено на 21 ноември 2026.

S53 МВР, предупреждение за фалшиви имейли с "призовки от полицията", 28 август 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. Проверено на 21 ноември 2026.

S54 МВР, беседа на служители по киберпрестъпност за отвлечени акаунти, 19 ноември 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. Проверено на 21 ноември 2026.

S56 МВР, участие в операция PowerOFF срещу услуги за DDoS под наем, 16 април 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. Проверено на 21 ноември 2026.

S58 CMS, "EU DORA Regulation amendments submitted to Bulgarian Parliament", 7 февруари 2025 (актуализирано на 24 септември 2026). https://cms.law/en/bgr/legal-updates/eu-dora-regulation-amendments-submitted-to-bulgarian-parliament. Проверено на 21 ноември 2026.

S59 Портал за обществени консултации на Министерския съвет, проект на Закон за устойчивостта на критичните субекти, консултация 27 май-26 юни 2025. https://www.strategy.bg/bg/public-consultations/11134. Проверено на 21 ноември 2026.

S60 Министерство на иновациите и дигиталната трансформация, решение на Министерския съвет за администрациите, включени в Националната система за киберсигурност, 4 ноември 2026. https://midt.gov.bg/bg/news/1604. Проверено на 21 ноември 2026.

S61 BTA, "Hacker attacks on government websites continue", изявление на министъра на иновациите и дигиталната трансформация, 19 ноември 2026. https://www.bta.bg/en/news/bulgaria/1250121-hacker-attacks-on-government-websites-continue-innovation-and-digital-transform. Проверено на 21 ноември 2026.

S62 Fakti, по информация на БНР, изявление на ръководителя на отдела за киберразузнаване в ГДБОП за измами с IBAN на получателя срещу фирми, 3 юни 2026. https://www.fakti.bg/en/bulgaria/1058695-gdbop-hakeri-iztochvat-milioni-ot-firmi-v-balgaria. Проверено на 21 ноември 2026.

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

S64 ENISA, *ENISA Threat Landscape* 2026, септември 2026. https://www.enisa.europa.eu/sites/default/files/2026-09/ENISA%20Threat%20Landscape%202026_Final.pdf. Проверено на 21 ноември 2026.

S65 Money.bg, материал за неоторизиран достъп до вътрешна система на хостинг доставчик (заглавието назовава компанията), 17 ноември 2026 (актуализиран на 18 ноември). https://money.bg/ (адресът на статията е пропуснат). Проверено на 21 ноември 2026.

S66 Sekoia, "Poisoned Source: APT29 watering holes target mobile devices with n-day exploits", 4 ноември 2026. https://www.sekoia.com/blog/poisoned-source-apt29-watering-holes-targets-mobile-devices-with-n-day-exploits; материал на български в Ruse.news, 5 ноември 2026: https://ruse.news/index.php/2026/11/05/kampaniya-za-kiberataki-vklyuchila-balgarski-sajt-ot-voennata-sfera/. Проверено на 21 ноември 2026.

S67 Fakti, препубликуван материал на Reuters за имейл кампания, приписвана от изследователи на APT28, достигнала пощенски кутии на местни служители в Пловдивска област, 15 април 2026. https://www.fakti.bg/ (URL на статията не се посочва). Проверено на 21 ноември 2026.

S68 CISA, ФБР и международни партньори, съвместно предупреждение AA25-343A, "Pro-Russia Hacktivists Conduct Opportunistic Attacks Against US and Global Critical Infrastructure", 9 декември 2025; препубликувано от NCSC на Нова Зеландия на 15 декември 2025. https://www.ncsc.govt.nz/alerts/pro-russia-hacktivists-conduct-attacks-against-critical-infrastructure. Проверено на 21 ноември 2026.

S69 KELA, "OT threat intelligence, part 2", актуализиран на 3 септември 2026. https://www.kelacyber.com/blog/ot-threat-intelligence-part2/. Проверено на 21 ноември 2026.

S70 Cyble, профил на рансъмуер групата Krybit, 22 септември 2026. https://cyble.com/threat-actor-profiles/krybit-ransomware-threat-actor/. Проверено на 21 ноември 2026.

S72 БНР (Радио България), "Wave of bomb threats paralyzes dozens of institutions across Bulgaria", 7 юли 2026. https://bnrnews.bg/en/post/499930/wave-of-bomb-threats-paralyzes-dozens-of-institutions-across-bulgaria. Проверено на 21 ноември 2026.

S73 Комисия за финансов надзор, английски текст на Закона за пазарите на криптоактиви, Държавен вестник, бр. 54 от 4 юли 2025. Преходните и заключителните му разпоредби изменят Закона за кредитните институции, Закона за платежните услуги и платежните системи (нов чл. 182б) и Закона за Комисията за финансов надзор във връзка с DORA. https://www.fsc.bg/wp-content/uploads/2026/01/markets_in_cryptoassets_act.pdf. Проверено на 21 ноември 2026.

Приложение D. Речник

- **Blackhole:** източник на данни за киберпрестъпността на Brandefense, който обхваща публикации, заразени устройства, идентификационни данни и данни за карти.
- **Ransompedia:** базата данни за рансъмуер на Brandefense; обявите записват твърдения на престъпници.
- **Atlas:** оценяването на външното излагане на Brandefense; оценките са от 0 (нищо не е наблюдавано) до 100.
- **Заразено устройство:** устройство, чийто stealer лог съдържа вход в домейна на организацията; „на служител" е класификация, а не проверена трудова заетост.
- **Обява на пазар за идентификационни данни:** идентификационни данни, свързани с домейна, предлагани на наблюдаван пазар към момента на проверката.
- **Combolist:** списък с двойки потребителско име и парола, събрани от различни източници; възрастта и валидността варират.
- **Stealer лог:** данни, събрани от устройство от зловреден софтуер за кражба на информация.
- **Checker бот:** бот, който тества откраднати карти срещу платежни шлюзове и отпечатва резултата.
- **Карта на публикация:** редактирано възпроизвеждане на една публикация от тъмната мрежа с място, дата, псевдоним, език и какво установява и какво не установява.
- **Препредаване:** канал или бот на трета страна, който публикува повторно твърдение на друг извършител; препредаването е по-слабо доказателство от собствената публикация на извършителя.
- **Публикация, специфична за България:** публикация, в която България е предметът, а не един от редовете в списък с няколко държави.
- **ЕГН:** българският личен идентификационен номер (единен граждански номер), присвояван на всеки гражданин.
- **IBAN:** международен номер на банкова сметка; българските IBAN започват с BG.
- **NIS2:** директивата на ЕС за високо общо ниво на киберсигурност (Директива (ЕС) 2022/2555), транспонирана в България чрез измененията от 2026 на Закона за киберсигурност.
- **Съществени и важни субекти:** двете категории обхванати организации по NIS2; за съществените субекти се прилага по-високият максимален размер на глобите.
- **Ранно предупреждение:** първото докладване на инцидент по NIS2, дължимо до 24 часа след откриване на значителен инцидент.
- **DORA:** Регламентът на ЕС за цифровата оперативна устойчивост на финансовите субекти.
- **CSIRT:** екип за реагиране при инциденти с компютърната сигурност; CERT България е националният екип.
- **DMARC / SPF / DKIM:** стандарти за удостоверяване на имейл; DMARC казва на получателите какво да правят с писмата, които не преминават проверката.
- **DNSSEC:** подписи, които позволяват на резолверите да проверяват DNS отговорите.
- **DS запис:** записът в родителската зона, който свързва домейна с неговите DNSSEC ключове.
- **HSTS:** уеб заглавка, която указва на браузърите да използват само HTTPS.
- **TLP:CLEAR:** може да се споделя без ограничение; другите законови задължения продължават да се прилагат.
- **BIN:** префиксът на номера на картата, определящ издателя (банков идентификационен номер).
- **KYC:** проверки на самоличността „познавай своя клиент" в банки, борси и други услуги.

- **Дропове и сметки на мулета:** хора и сметки, открити на тяхно име, използвани за получаване и прехвърляне на средства от измами.
- **Smishing:** фишинг чрез SMS или приложение за съобщения.
- **Домейн имитатор:** домейн, регистриран така, че да прилича на домейна на реална организация, използван за фишинг.
- **MFA (многофакторно удостоверяване):** вход, който изисква втори фактор освен паролата.
- **Устойчиво на фишинг MFA:** вход, обвързан с истинския сайт (ключове за сигурност FIDO2, passkeys или сертификати), така че препредаваща страница не може да го използва повторно.
- **OT:** операционни технологии, системите, които управляват физически процеси; операторският панел е техният локален екран за управление.
- **Web shell:** скрипт, поставен на уеб сървър, който дава на нападателя отдалечен контрол над него.
- **Обобщаваща оценка:** националната стойност на Atlas за всичките 250 организации (50 от 100; по-високо означава по-голяма експозиция).
- **p=none:** политика DMARC, която само наблюдава и не изисква от получателите да отхвърлят писмата или да ги поставят под карантина.
- **Индекс на пасивната хигиена:** аналитичен композитен показател на Odin от проверки на имейл, DNS, TLS и заглавки; 0–100, по-висока стойност означава по-слаба хигиена.
- **RTO:** целево време за възстановяване, най-дългото прекъсване, което планът за непрекъснатост допуска.
- **3-D Secure:** еднократният код или потвърждението в приложение, които издателят на картата изисква при онлайн плащане.
- **SCADA:** система за надзорно управление и събиране на данни, софтуер за наблюдение и управление на промишлени процеси; Rapid SCADA е един продукт с отворен код.
- **VNC:** протокол за отдалечен работен плот; изложените VNC връзки дават отдалечен контрол над екрана.
- **SSRF:** фалшифициране на заявки от страна на сървъра, уязвимост, при която сървърът изпраща заявки от името на нападател.
- **CAA запис:** DNS запис, който посочва кои удостоверяващи органи могат да издават сертификати за домейна.
- **CMS:** система за управление на съдържанието, софтуерът, на който работи даден сайт.
- **APT28 / APT29:** имена, които доставчиците на сигурност използват за две шпионски групи; приписването във всеки случай е на източника, а не наше.
- **База с контакти:** списък с лични контактни данни, продаван за маркетинг или измами.

За този доклад

Изготвен от Odin by Brandefense. Версия 1.0 е завършена на 21 ноември 2026.

Краен срок на изследването: 18 ноември 2026 (основен период на данните); официалните и медийните материали са прочетени до 21 ноември 2026 (**Приложение А.8**). Докладът дава приоритет на собствените данни на Brandefense, разграничава твърденията на престъпници от независимо установените инциденти и не претендира за пълно преброяване на киберпрестъпността, засягаща България. Препоръките описват какво биха могли да направят организациите; те не твърдят, че дадена организация ги е изпълнила или не. Авторите не заемат позиция по българската или международната политика; официалните изявления и приписвания се предават така, както ги е дал източникът. Това издание на български език придружава изданието на английски; при разлики предимство има изданието на английски език.

© 2026 Brandefense. Всички права запазени.