HACKOUT | Portalul Atacurilor Cibernetice

Bulgaria NRA
National Revenue Agency

Introducere

Atacul a fost lansat în luna Iulie a anului 2019 asupra Bulgaria NRA (National Revenue Agency), echivalentul ANAF în România. Acesta este unul dintre cele mai cuprinzătoare leak-uri de date de pe teritoriul Bulgariei, fiind afectate atât instituțiile de fiscalitate și finanțe ale statului bulgar cât și cetățenii acestuia. În acest atac au fost furate nume, date personale şi declaraţii fiscale ale unor persoane şi întreprinderi.

În centrul acestei anchete se află compania Tad Group, Kristian Boykov, fiind singura persoană acuzată până acum pentru implicarea în atacul cibernetic asupra Agenției Fiscale. Boykov, în vârstă de 20 de ani, a negat acuzațiile, fiind apoi eliberat, dar acesta primind interdicția de a părăsi țara.

Mai multe canale informative din Romania au scris despre această informație la data respectivă.

Șeful unei companii IT, reținut după ce hackerii au furat de la Fiscul bulgar datele a 5 milioane de oameni

Sursa: digi24.ro

Furt istoric de date de la Fiscul bulgar: Guvernul suspectează un atac motivat politic. Cine sunt suspecţii şi ce glumă au făcut pe seama autorităţilor de la Sofia

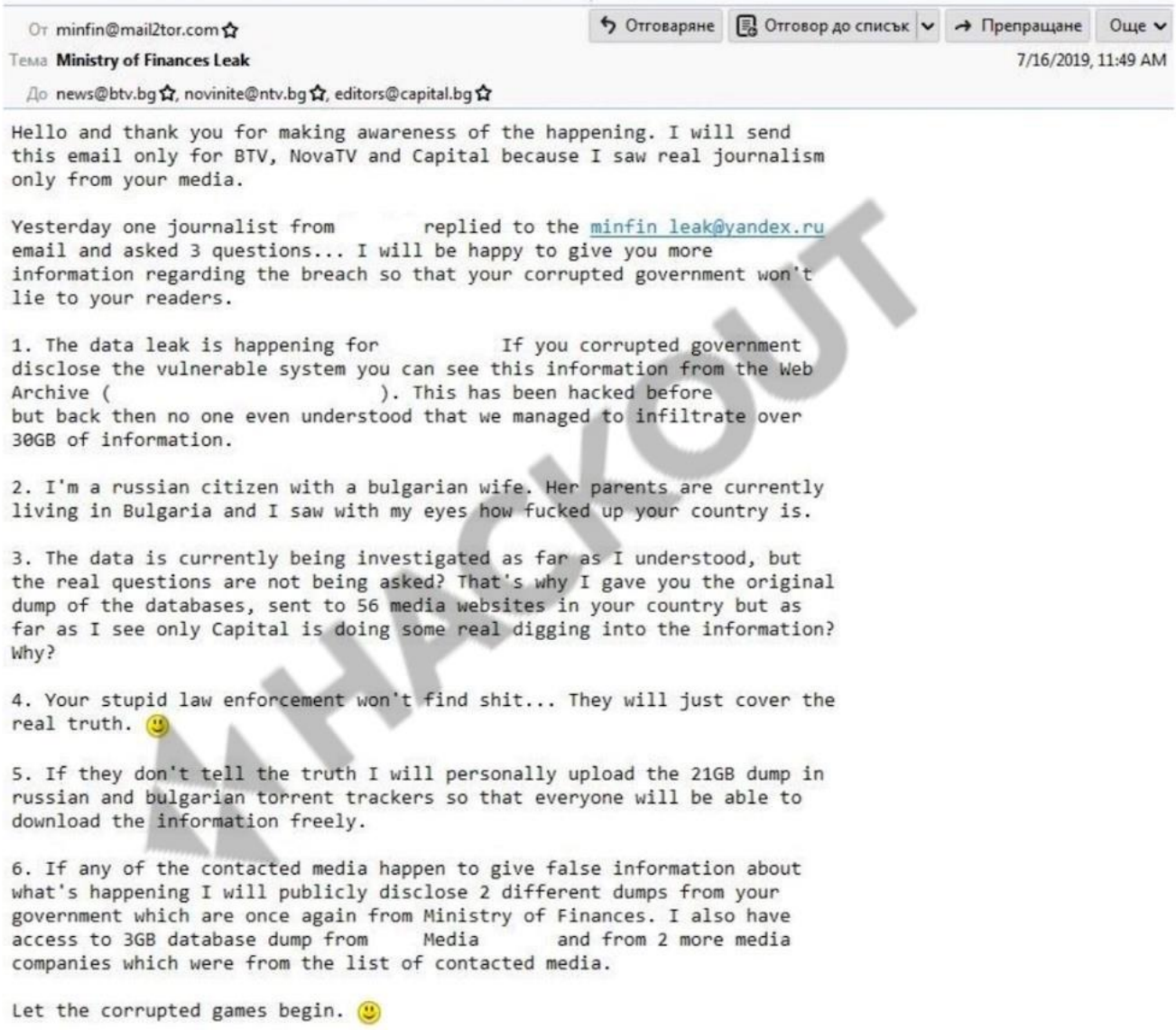
Sursa: adevarul.ro

Agenția Fiscală se confruntă cu o amendă de 20 de milioane de euro în urma breșei de securitate, despre care oficialii au declarat că a fost compromisă aproximativ 3% din baza de date a agenției. Scurgerea de informațiii include de asemenea fișele agenției europene anti-fraudă EUROFISC, care permite administrațiilor fiscale naționale să distribuie informații legate de activitățile ilegale și pentru combaterea fraudelor în materie de TVA.

Datele nearhivate ocupă un spațiu de aproximativ **11 GB**, organizate în **57** de foldere ce conțin **1044** de fișiere cu extensia .csv .

Sursa datelor

Hacker-ul responsabil pentru această breșă a trimis mail-uri trusturilor de presă bulgare despre scopul atacurilor împreună cu leak-ul atașat, susținând că întregul leak are o dimensiune de aproximativ 21 GB și 110 foldere. Chiar și așa, cei 11 GB care au fost făcuți public pe forumul RaidForum conțin datele personale (nume, CNP, tranzacții bancare, informații despre pensii și conturi curente la diferite bănci, informații despre utilizatori ai unor site-uri de jocuri de noroc online etc.) ale aproximativ 5 milioane de cetățeni bulgari și nu numai. Se vehiculează faptul că toate persoanele adulte din statul bulgar au fost afectate de către acest leak.



От minfin@mail2tor.com

Отговаряне | Отговор до списък | Препращане | Още

Тема **Ministry of Finances Leak** 7/16/2019, 11:49 AM

До news@btv.bg, novinite@ntv.bg, editors@capital.bg

Hello and thank you for making awareness of the happening. I will send this email only for BTV, NovaTV and Capital because I saw real journalism only from your media.

Yesterday one journalist from replied to the minfin_leak@yandex.ru email and asked 3 questions... I will be happy to give you more information regarding the breach so that your corrupted government won't lie to your readers.

1. The data leak is happening for If you corrupted government disclose the vulnerable system you can see this information from the Web Archive ( ). This has been hacked before but back then no one even understood that we managed to infiltrate over 30GB of information.

2. I'm a russian citizen with a bulgarian wife. Her parents are currently living in Bulgaria and I saw with my eyes how fucked up your country is.

3. The data is currently being investigated as far as I understood, but the real questions are not being asked? That's why I gave you the original dump of the databases, sent to 56 media websites in your country but as far as I see only Capital is doing some real digging into the information? Why?

4. Your stupid law enforcement won't find shit... They will just cover the real truth.

5. If they don't tell the truth I will personally upload the 21GB dump in russian and bulgarian torrent trackers so that everyone will be able to download the information freely.

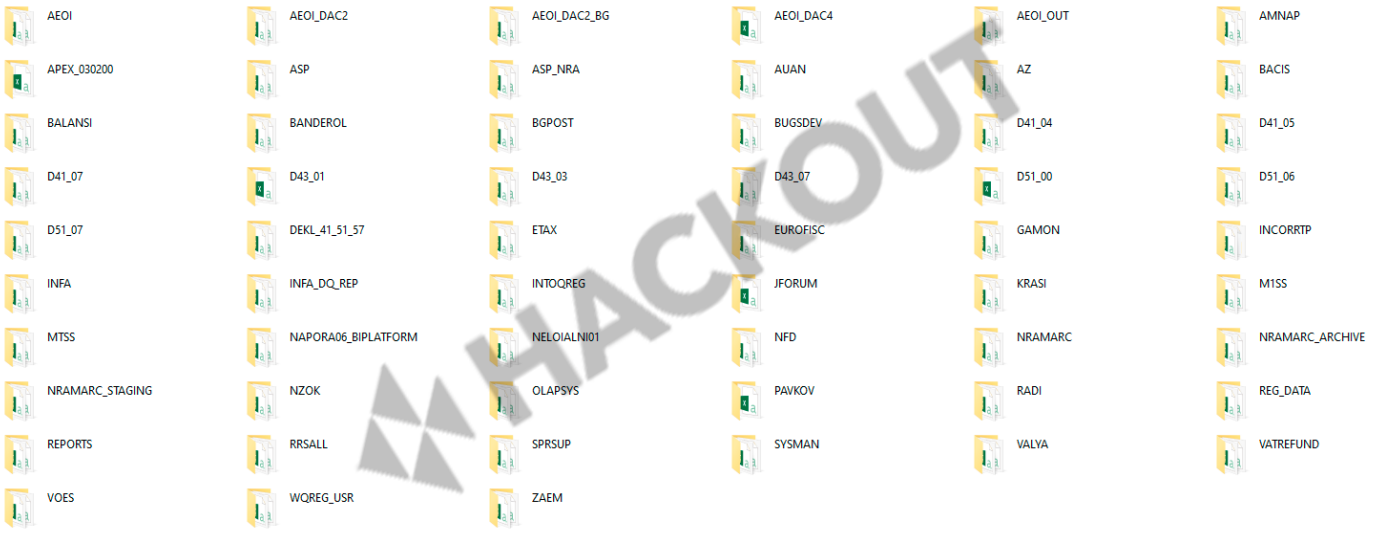
6. If any of the contacted media happen to give false information about what's happening I will publicly disclose 2 different dumps from your government which are once again from Ministry of Finances. I also have access to 3GB database dump from Media and from 2 more media companies which were from the list of contacted media.

Let the corrupted games begin.

HACKOUT

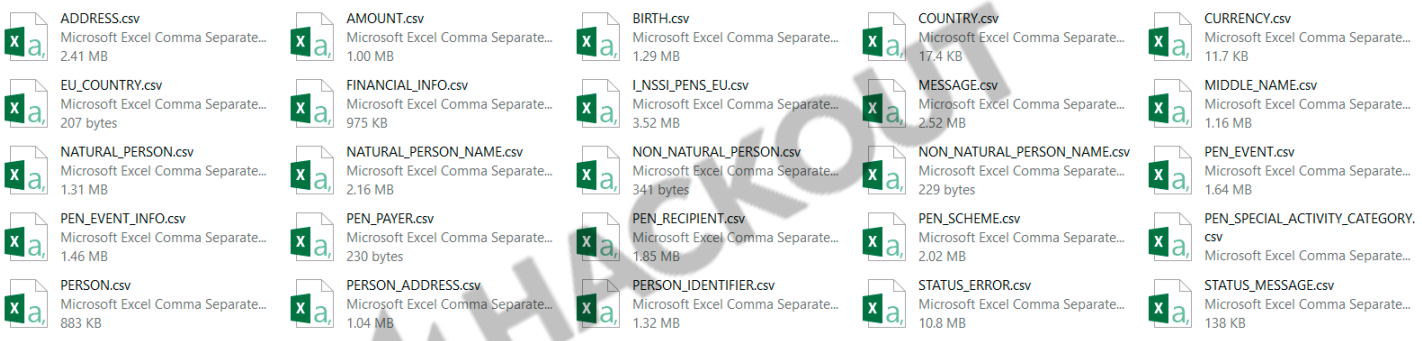
Altă informație din spațiul public (*cyberscoop.com*) descrie autorul incidentului ca fiind un contractor al guvernului bulgar (Kristian Boykov, 20 de ani), specialist în securitate cibernetică implicat în testarea și auditul sistemelor informatice. Se presupune că acesta a exploatat o vulnerabilitate într-un serviciu de rambursare a TVA-ului pentru tranzacții externe, un serviciu rar folosit și neactualiza

Cele 57 de foldere:



Folderele sunt organizate pe instituții, aplicații sau servicii oferite de instituțiile respective, de exemplu VATREFUND, un serviciu folosit pentru deducerea de TVA.

Structura unui folder:



Fișierele .csv din fiecare folder au numele unor tabele din baza de date a instituției respective sau a serviciului respectiv.

Cel mai probabil, hackerul a luat fiecare tabel în parte și le-a exportat în format CSV apoi le-a împartit pe aplicații/servicii folosind structura folderelor.

Ce ne propunem

În acest articol ne propunem o analiză amănunțită a ceea ce reprezintă date de interes pentru organizațiile și persoanele fizice din România ce desfășoară sau au desfășurat activități comerciale/fiscale/sociale pe teritoriul Bulgariei în perioada 2007 - Iulie 2019 (perioada afectată de datele făcute publice). Aceste date pot reflecta breșe majore la nivelul societăților comerciale cu răspundere limitată (SRL), dar și la nivel personal, pentru cetățenii români.

Conținutul:

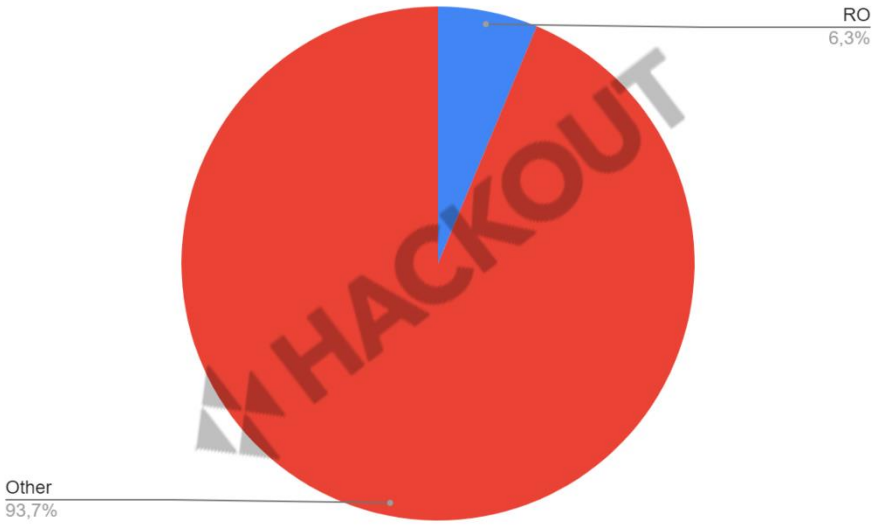
În total, fișierele conțin aproximativ **72,600** de înregistrări ce fac referire la tranzacțiile dintre numeroase firme românești ce se ocupă cu jocurile de noroc, dar și mail-urile angajaților acestora. Printre aceste înregistrări se regăsesc si firme mari de transporturi de pe teritoriul României.

lines : 72,597 | Ln : 1 | Col : 1 | Sel : 0 | 0

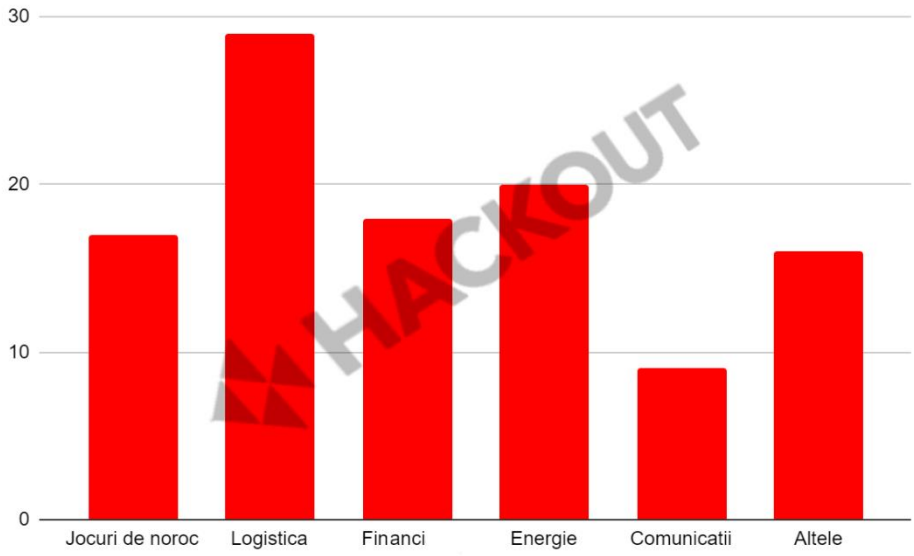
Folderul AEOI:

Acesta conține numeroase legături cu entitați fizice sau juridice, acestea aparținând teritoriului României, acestora findu-le publicate date personale, conturi, etc.

Dintre aceste date **13** persoane figureaza in sectorul de **pensii**.

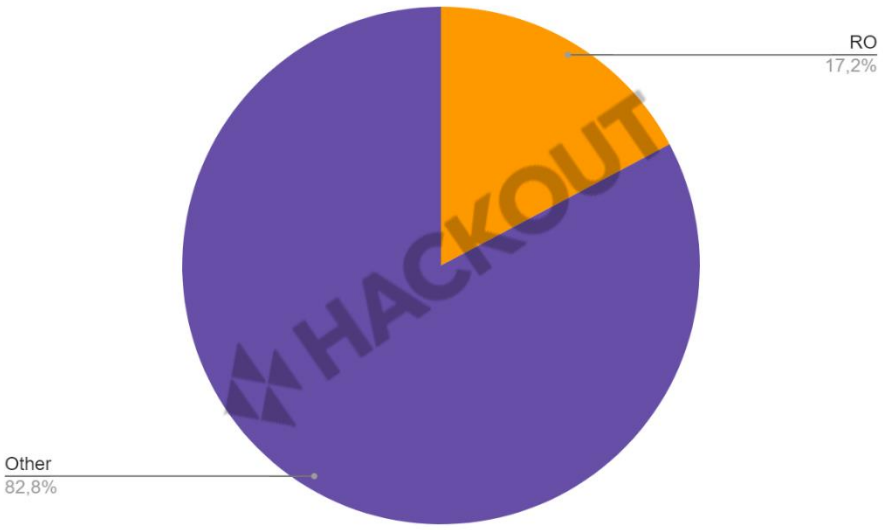


Circa **1480** de **firme** de pe teritoriul **României** au fost implicate în tranzacții, ce figurează în acest leak de pe teritoriul Bulgariei, acesta expunându-le atât identitatea cât și obiectul de activitate.



Folderul AEOI_DAC2:

Contine circa **3542** de nume de persoane, acestea fiind identificate cu codul de legatura RO: 191. De asemenea acest folder desfasoară numeroase date personale ale acestor români.

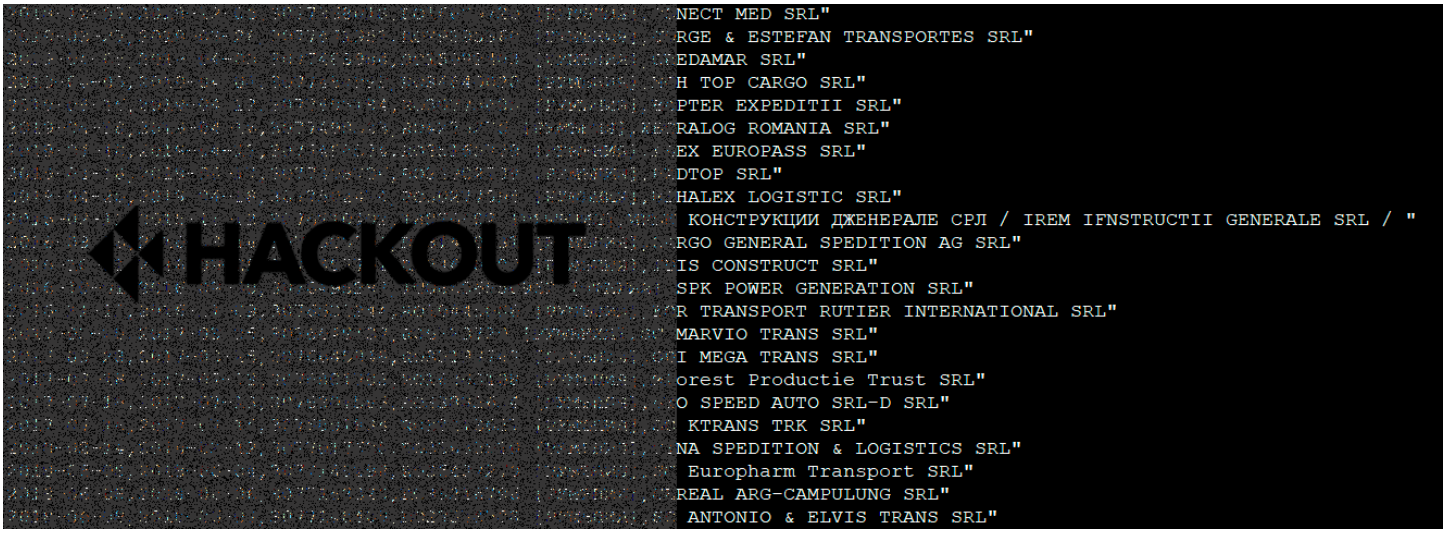


Folderul AEOI_DAC2_BG:

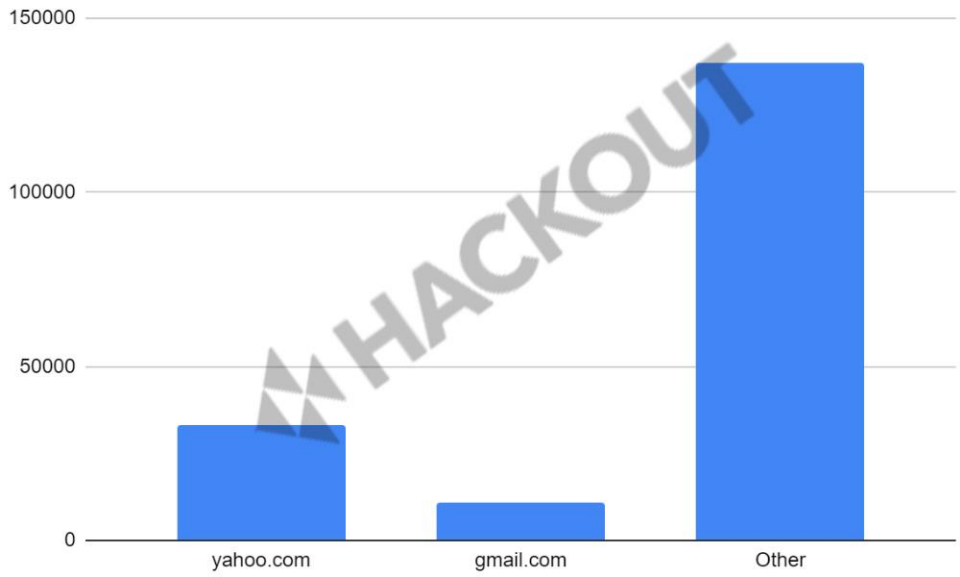
Contine aproximativ **9357** de adrese de email din România, precum și date personale a **7950** români în subdirectorul: AEOI_DAC2_COUNTRY_Message , **3883** persoane de naționalitate română în subdirectorul : _H.csv.

Folderul BACIS:

Conține informații cu privire la tranzacțiile a **1605** firme românești pe teritorul Bulgariei.



În total au fost identificate circa **181.563** adrese de **Gmail**, dintre care **10.863** de adrese aparțin persoanelor sau firmelor **românești**, **33.269** adrese de **Yahoo**, dintre care **1.848** adrese aparțin unor persoane sau firme de pe teritoriul **Romaniei**.



În ce procentaj au fost afectate persoane de cetățenie română prin acest leak: 8,5%

Bulgaria

Aceasta pe de altă parte a suferit o adevarată breșă de securitate: peste 1.300 de conturi guvernamentale și mailuri au fost publicate, alături de nume, adrese și chiar parole.

Marea majoritate a adreselor de mail aparțin domeniului nra.bg dar și a subdomeniilor aferente acestuia

uganski@ro15.nra.bg
v@ro03.nra.bg
ieva@ro03.nra.bg
tantinova@ro03.nra.bg
@ro22.nra.bg
a@ro22.nra.bg
dzhieva@ro22.nra.bg

ova@ro29.nra.bg
nibov@ro03.nra.bg
ov@ro03.nra.bg
rdzhieva@ro03.nra.bg

În total, sunt peste 1.400.000 de rânduri de tabel, zeci de țări, mii de mailuri și parole expuse (chiar și în clar text).

Concluzie

În ciuda aparițiilor media ale acestui incident și a impactului asupra cetățenilor români, nu există dovezi care să ridice un semn de alarmă. Datele sunt în mare parte financiare, diferite sume ce reprezintă cotizații către bugete, contribuții către pensii, plăți TVA etc.

Asadar, această breșă de securitate afectează exclusiv funcționarii publici din Bulgaria și integritatea conturilor acestora precum și a câtorva firme ale căror nume sunt prezente în leak.