HACKOUT | Portalul Atacurilor Cibernetice

Collection#1-#5

https://hackout.ro

1.Cuvânt înainte

Hackout.ro este un portal în care sunt publicate atacurile cibernetice ce vizează și cetățeni români, websiste-uri din România și tot ce ține de România pe plan cibernetic. Scopul principal al portalului este cel de informare a cetățenilor, sporirea vigilenței acestora, dar și servicii gratuite destinate utilizatorilor.

Cu ajutorul platformei utilizatorii pot: verifica dacă conturile lor au fost compromise în trecut, verifica cât de sigure sunt parolele, monitoriza e-mailurile și website-urile, afla informații noi și învăța termenii cyber – security, vizualiza statistică și rapoartele periodice și, mai ales, pot cere asistență gratuită pentru rezolvarea incidentelor cibernetice.

Scopul acestui raport este menținerea unui grad ridicat de alertă în rândul cetățenilor, dar și conștientizarea pericolului la care se expun în momentul în care își folosesc mailurile instituționale sau de serviciu în fața atacurilor cibernetice ce vizează în mod direct obținerea bazei de date a respectivei platforme/website, precum și a datelor personale existente în aceasta.

Raportul a fost întocmit în luna aprilie 2019, iar datele au fost analizate în decursul a primelor trei luni din același an. Toate datele prezentate au caracter orientativ. Nu răspundem de exactitatea acestora și nici de a posibilelor erori ce pot apărea.

Datele au fost analizate în mod automat, fără a se interveni asupra lor. Datele personale și parolele utilizatorilor nu au fost utilizate și nici accesate decât prin instrumente software adecvate ce respectă normele de protecție a datelor cu caracter personal conform legii 506/2004, precum și a legilor ce vin în completarea acesteia.

Efortul depus în realizarea acestui raport este unul colectiv, toată investiția de timp și resurse este strict personală a echipei ce a dus la bun sfârșit această analiză. Nu au existat alte părți investiționale în afară de echipa realizatoare a acestui studiu, iar scopul nu este altul decât informarea și educarea cetățenilor.

Toate ipotezele, concluziile, observațiile și explicațiile sunt subiective, nu ne asumăm niciun fel de răspundere asupra lor.

ULTERIOR:

E îmbucurător pentru noi faptul că o parte a presei din România acordă atenție subiectelor legate de domeniul securității cibernetice, preluând inclusiv studiul nostru.

Însă, pentru corecta informare și întelegere a mesajului pe care am încercat să-l transmitem prin intermediul acestui studiu, dorim să facem câteva precizări suplimentare:

Colectarea datelor invocate în studiu s-a făcut în perioada ianuarie-aprilie 2019, însă conține inclusiv date ce aparțin unor leak-uri mai vechi, ceea ce înseamnă că unele dintre acestea nu mai sunt de actualitate.

Un alt aspect care trebuie subliniat este acela că site-urile instituțiilor publice menționate în studiu nu au fost compromise (așa cum reiese din unele articole din presă care fac trimitere la studiul nostru).

Spre exemplificare, site-ul gov.ro (dar și celelalte) nu a fost compromis, însă există situații în care persoane ce dețin conturi de mail asociate acestui domeniu au folosit conturile respective pentru accesarea unor site-uri compromise la un moment dat.

Acesta este motivul pentru care atragem atenția cu privire la folosirea mailurilor profesionale pentru accesarea altor platforme, aplicații sau site-uri în afara celor pentru care au fost destinate inițial.În caz contrar, contul de mail al utilizatorului este expus.

Din acest considerent este important, pentru sporirea securității conturilor utilizatorilor să nu folosească aceeași parola pentru mai multe tipuri de servicii.

Recomandăm în continuare folosirea instrumentelor de pe pagina de verificare pentru a afla dacă mailul sau parola dvs. sunt compromise dar și consultarea paginii de informare pentru a afla cum îți poți seta o parolă puternică și cum te poți proteja pe internet!

2.Cuprins

3.Introducere

- Collection#1 + Antipublic#2...#5 –

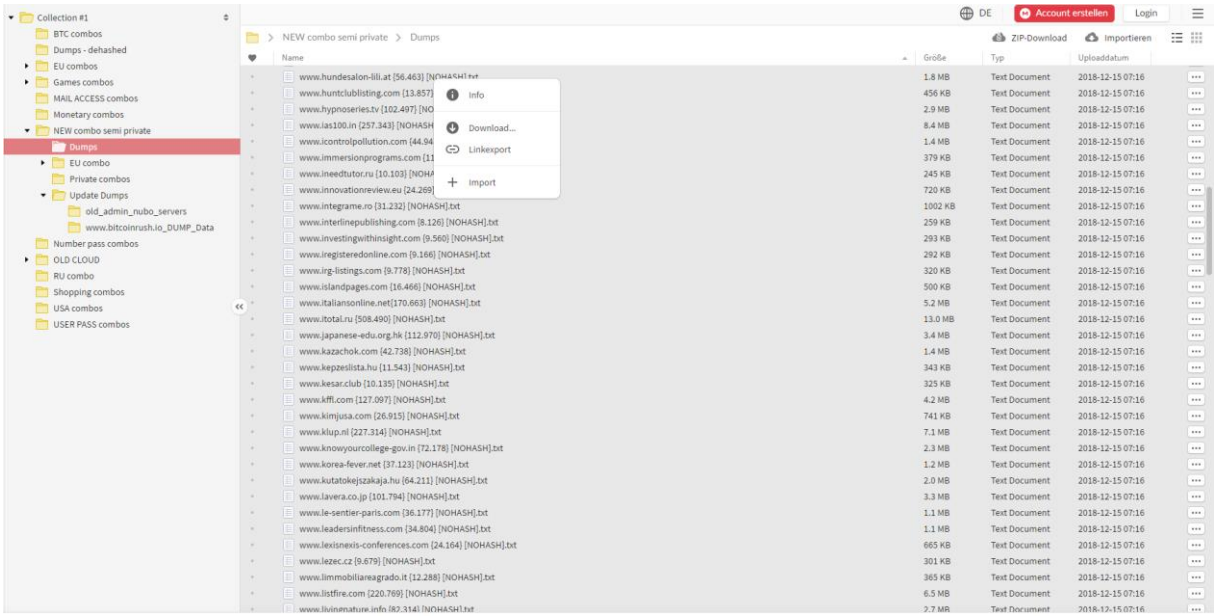
Collection#1 (care cuprinde 5 subcolecții) este unul dintre **cele mai mari leak**-uri apărute pe internet, cel puțin dintre cele ce au fost făcute publice.

(Un **leak** -> reprezintă datele sustrase din diferite sisteme în urma unei breșe de securitate, date printre care se numară e-mailuri, nume de utilizatori, parole, numere de telefon, adrese etc.)

Datele arhivate ocupă în total aproximativ 380 GB, iar dezarhivate mai multe de 2TB +.

Sursa datelor

Sursa datelor este una incertă, ele au fost pomenite prima dată pe blogul lui Troy Hunt, fondatorul HIPB. El povestește cum a găsit pe internet un cloud MEGA făcut public printr-un link. Acolo a găsit aproape 1TB de leak-uri, aceste date sunt acum considerate a fi Collection#1. Restul de #2 până la #5 se numesc Anti Public Combo List, acestea sunt dintr-o altă sursă, dar din cauza similarității structurii lor au fost puse în ,,aceeași oală” cu Collection#1. Diferiți experți ce au analizat sursa lor au afirmat chiar și faptul că ar putea avea același autor.

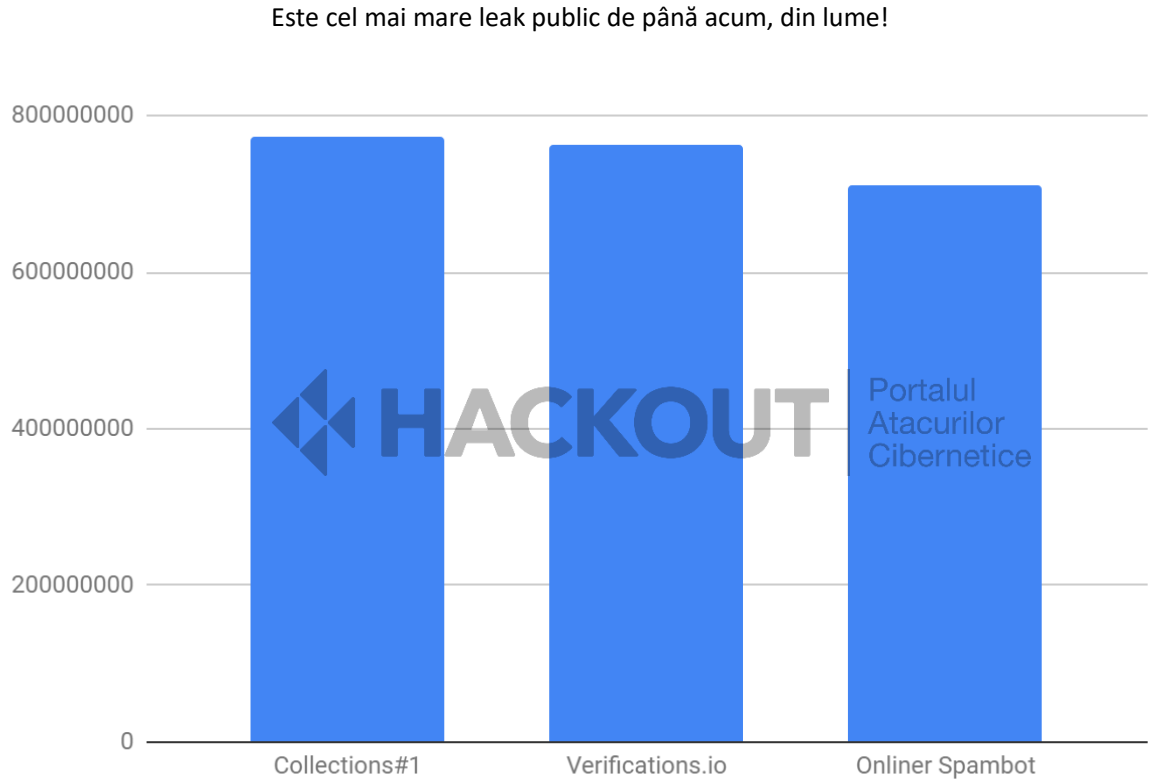


Poza aparține blogului lui TroyHunt www.troyhunt.com și ilustrează cloudul în care a găsit datele.

Ce ne propunem

În acest articol ne propunem să analizăm pe rând toate subcolecțiile, adică folderele: Collection#1, Collection#2,....,Colection#5; și să ajungem la o concluzie asupra importanței datelor și conținutul lor, dar şi riscul pe care îl reprezintă pentru utilizatorii din România .

În primul rând, sursa acestei arhive extrem de mare, este înca una **necunoscută**. Aceasta a fost postată pentru prima dată pe un forum din strainatate (RaidForum), forum cu un istoric bogat în acest domeniu. Arhivele sunt postate de mai multe ori, unele ,,raw"(date neprelucrate), altele chiar filtrate și re-organizate de diferiți oameni, altele sunt arhivate cu diferiți algoritmi pentru a optimiza dimensiunea acestora.



Așadar, posibilitățile sunt multiple. Pe Reddit mai mulți utilizatori au diferite ipoteze: arhiva a fost licitată pe un site, apoi vândută de la persoane la persoane până când și-a pierdut valoarea și a fost publicată pe internet *for free*; o altă versiune spune că arhiva ar fi fost gasită din pură coincidență; iar cea mai ,,votată" opțiune este cea care implică o grupare foarte mare, cu resurse de nivelul unui actor statal, provenind din partea est-europeană.

Am inceput analiza si am fost uimiți. Prioritatea noastră sunt insituțiile din Romania, cetațenii romani și tot ce ține de România.

4.Collection#1

Conținutul

Reprezintă în sine un leak separat fata de **Antipublic #2 - #5** , **Collection#1** are aprox 36GB arhivat și conține **milioane de conturi** sau combo-uri.

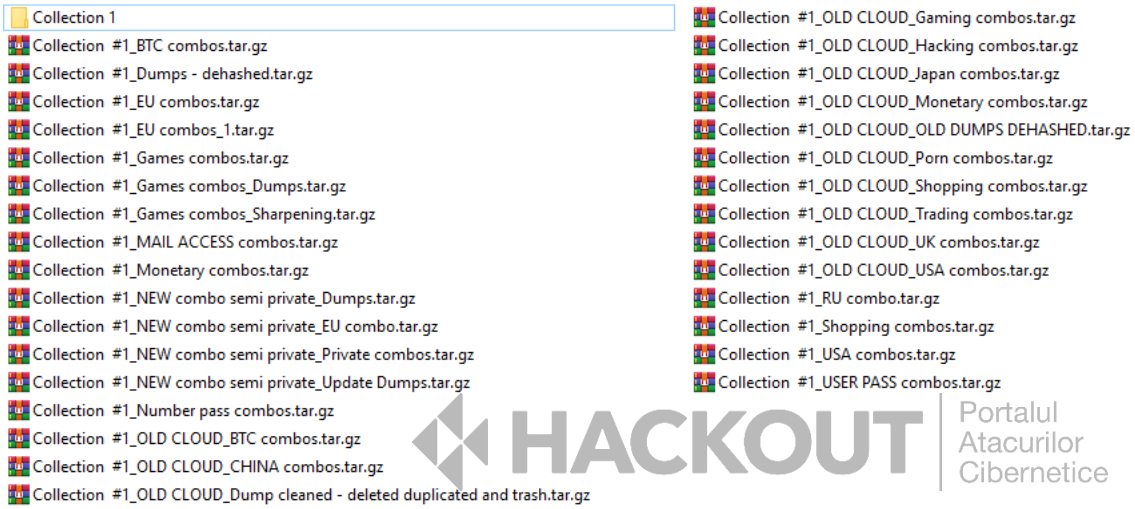
Adică 2,692,818,238 de rânduri în total.

El este alcătuit din punerea laolaltă a câtorva alte mii de leak-uri, breșe și date.

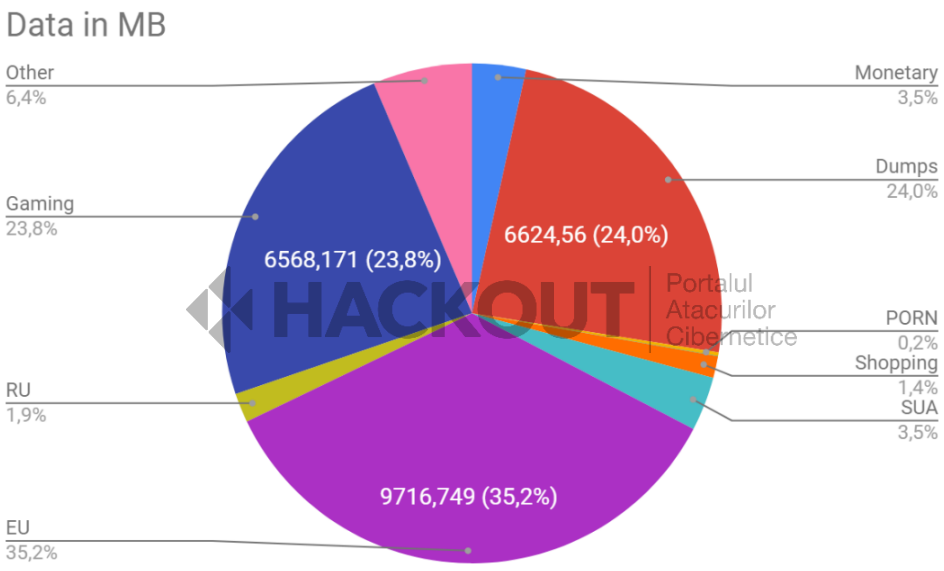
În total sunt **1,160,253,228** de combinații unice de mailuri și parole sau alte date cu caracter personal.

12,000 de fișiere în total.

Folderul conține **32 de arhive** care dezarhivate ating dimensiunea de **110GB**.



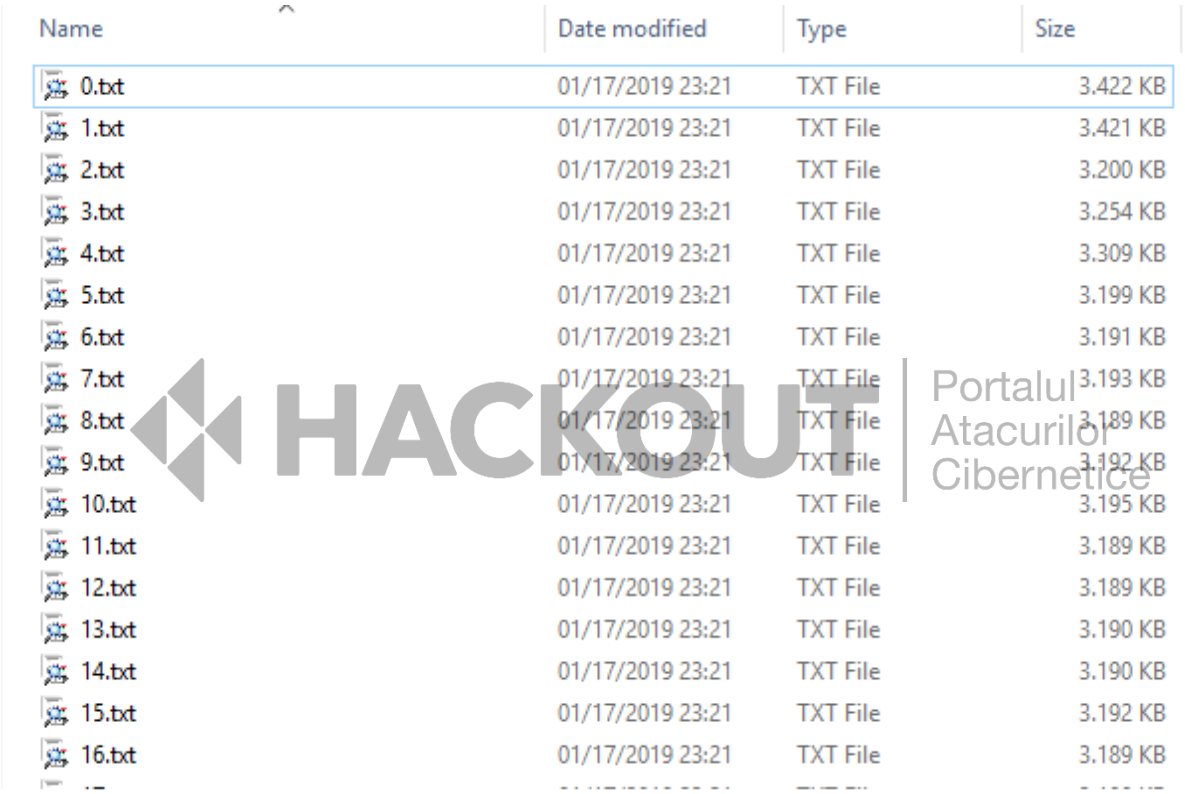
Pentru a putea clasifica mai bine datele, le-am împarțit pe domenii relevante și am obținut asta:



(dimensiunile sunt cele arhivate)

Lucrurile încep să devina interesante. Putem observa că cele mai multe date sunt **Dump**-uri, adică baze de date neprelucrate, în format brut (SQL) direct extrase din website-uri compromise, conturi și date de **Gaming** și conturi **EU**, adică mailuri și parole ale cetațenilor, parlamentarilor, funcționarilor publici europeni.

Fiecare arhivă/folder: conține fișiere numerotate de la 0, au extensia .txt și dimensiunea fiecăruia este de 3.09 MB. Cel mai probabil ele au fost împărțite astfel pentru a se caută mai ușor printre ele, iar dimensiunea a fost setată la 3 MB pentru a putea deschide fiecare fișier în parte cu orice fel de editor de text.



Name	Date modified	Type	Size
0.txt	01/17/2019 23:21	TXT File	3.422 KB
1.txt	01/17/2019 23:21	TXT File	3.421 KB
2.txt	01/17/2019 23:21	TXT File	3.200 KB
3.txt	01/17/2019 23:21	TXT File	3.254 KB
4.txt	01/17/2019 23:21	TXT File	3.309 KB
5.txt	01/17/2019 23:21	TXT File	3.199 KB
6.txt	01/17/2019 23:21	TXT File	3.191 KB
7.txt	01/17/2019 23:21	TXT File	3.193 KB
8.txt	01/17/2019 23:21	TXT File	3.189 KB
9.txt	01/17/2019 23:21	TXT File	3.192 KB
10.txt	01/17/2019 23:21	TXT File	3.195 KB
11.txt	01/17/2019 23:21	TXT File	3.189 KB
12.txt	01/17/2019 23:21	TXT File	3.189 KB
13.txt	01/17/2019 23:21	TXT File	3.190 KB
14.txt	01/17/2019 23:21	TXT File	3.190 KB
15.txt	01/17/2019 23:21	TXT File	3.192 KB
16.txt	01/17/2019 23:21	TXT File	3.189 KB

Fiecare fișier are fix 100.000 de linii, adică 100.000 de combo-uri.

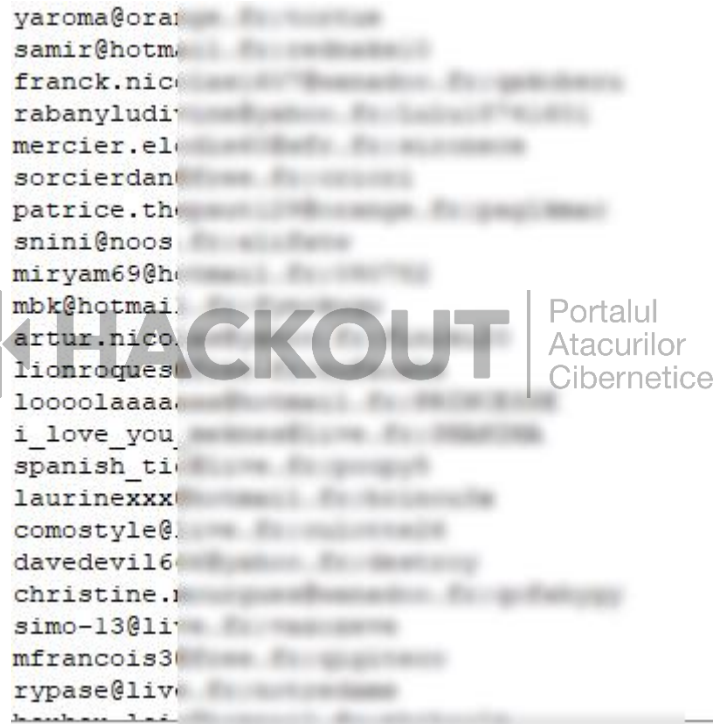
Din informațiile pe care le-am extras din meta-urile acestor fișiere, credem că arhivele au fost create și datele au fost restructurate/rearanjate în acest format la jumătatea lunii ianuarie 2019, când au apărut în spațiul public. Acest lucru este posibil să fii fost realizat de către un utilizator al forumului unde au fost găsite, pentru a ușura căutarea prin ele de către ceilalți utilizatori.

DUMP-uri si COMBO-uri

Trebuie precizat de pe acum faptul că toate arhivele conțin două tipuri de date:

1) **DUMPS** = fișiere format SQL cu toate informațiile și structura bazei de date de pe un anumit site
2) **COMBOS** = date în plaintext (text simplu, lizibil, format clar, fără criptare) ce reprezintă conturi, formatul este **mail:parola**

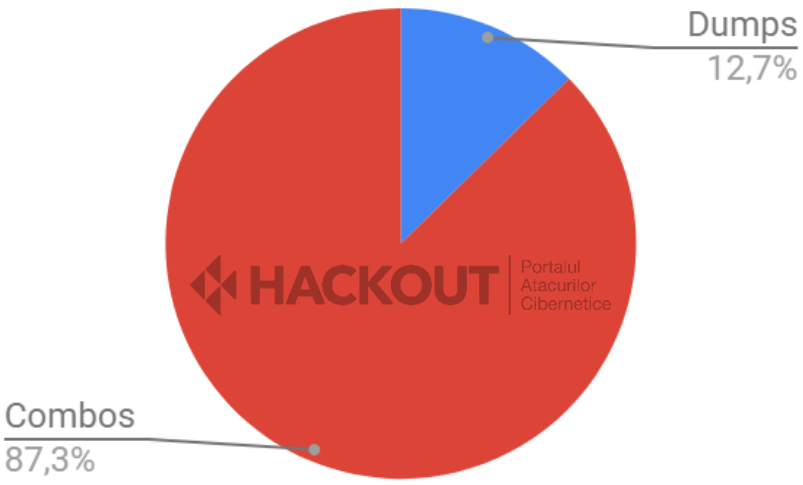
In cazul nostru, formatul este unul CSV adica **camp1;camp2**.



Exista însă mai multe tipuri de format adoptate, în diferite fișiere. Este un haos.

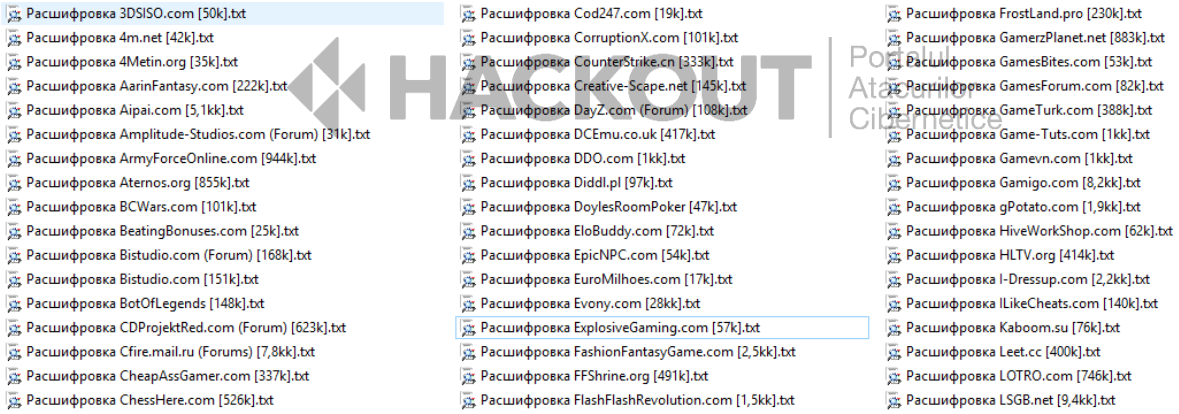
În total am găsit **772,904,991** de adrese de e-mail unice si **21,222,975** de parole unice (adică le-am numărat o singură dată, chiar dacă ele apăreau pentru mai multe conturi).

Analizând **natura datelor**, avem un procent semnificativ reprezentat prin combo-uri, fără să știm sursa lor și doar un procent de 12.7% de date de tip DUMP, despre care putem află de unde provin.



DUMP-uri

Analizând folderele cu dump-uri, regăsim sute de forumuri de gaming și jocuri.

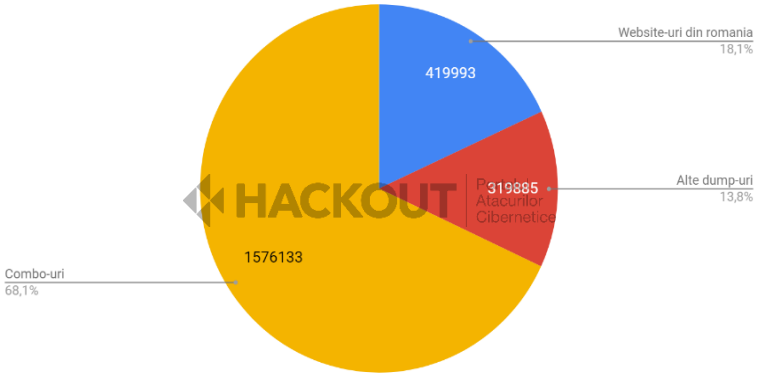


Din **România** figurează doar următoarele site-uri:

- Intergame.ro
- Experimental.ro
- Vacantesicalatorii.ro
- Secpral.ro
- Legisplus.ro
- Ktd.ro
- Experts.ro
- Irecson.ro
- Sferajuridica.ro
- Macheteshop.ro
- Ase.ro
- Biocom-international.ro
- Kgb-hosting.ro
- Propack-romania.ro
- Meteopress.ro
- Mobotix.ro
- Transindex.ro
- Jobstore.ro
- Jobee.ro
- Granturi.ro
- Rnt.ro
- Cartestraina.ro
- Linkweb.ro
- Psihologieonline.ro
- My-press.ro

În total, doar din acestea regăsim **410.933** conturi compromise ale utilizatorilor din Romania ce provin din website-uri românesti.

În total, avem **2.316.011** conturi unice din Romania, distribuite astfel:



Recapitulare

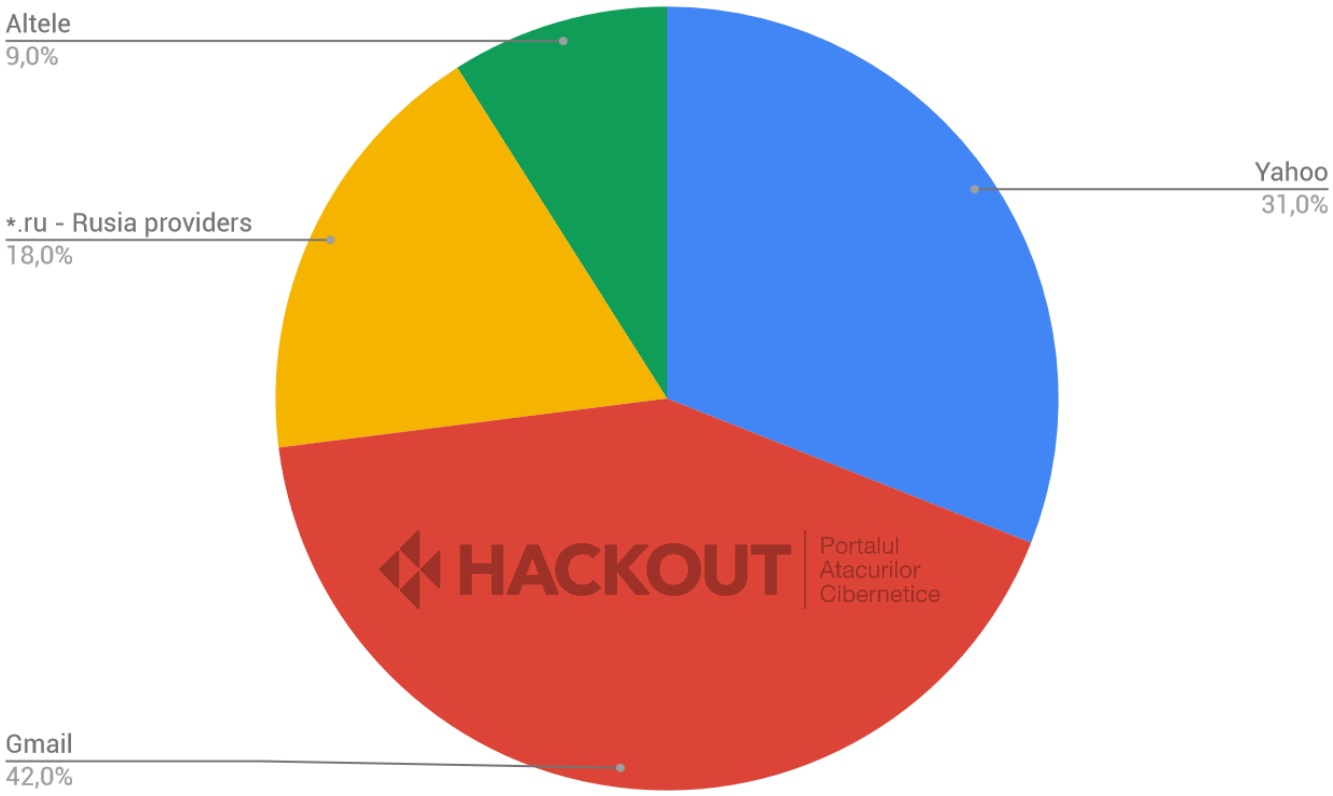
Avem **1,160,253,228,** din care românești sunt doar **0,2%**, adică **2,316,011.** Dintre acestea 68.1% au origini necunoscute, **18.1% provin din baze de date ale unor site-uri românești compromise** (25 de site-uri) si 13.8% din baze de date ale unor site-uri din afara României.

Un lucru demn de menționat este faptul că în toată ,,colecția" regăsim într-un procent foarte ridicat descrieri, nume de fișiere, explicații si instrucțiuni, toate în limba **rusă**.

Putem spune că se confirmă ipoteza mai multor utilizatori Reddit de la început referitoare la proveniență atacurilor.

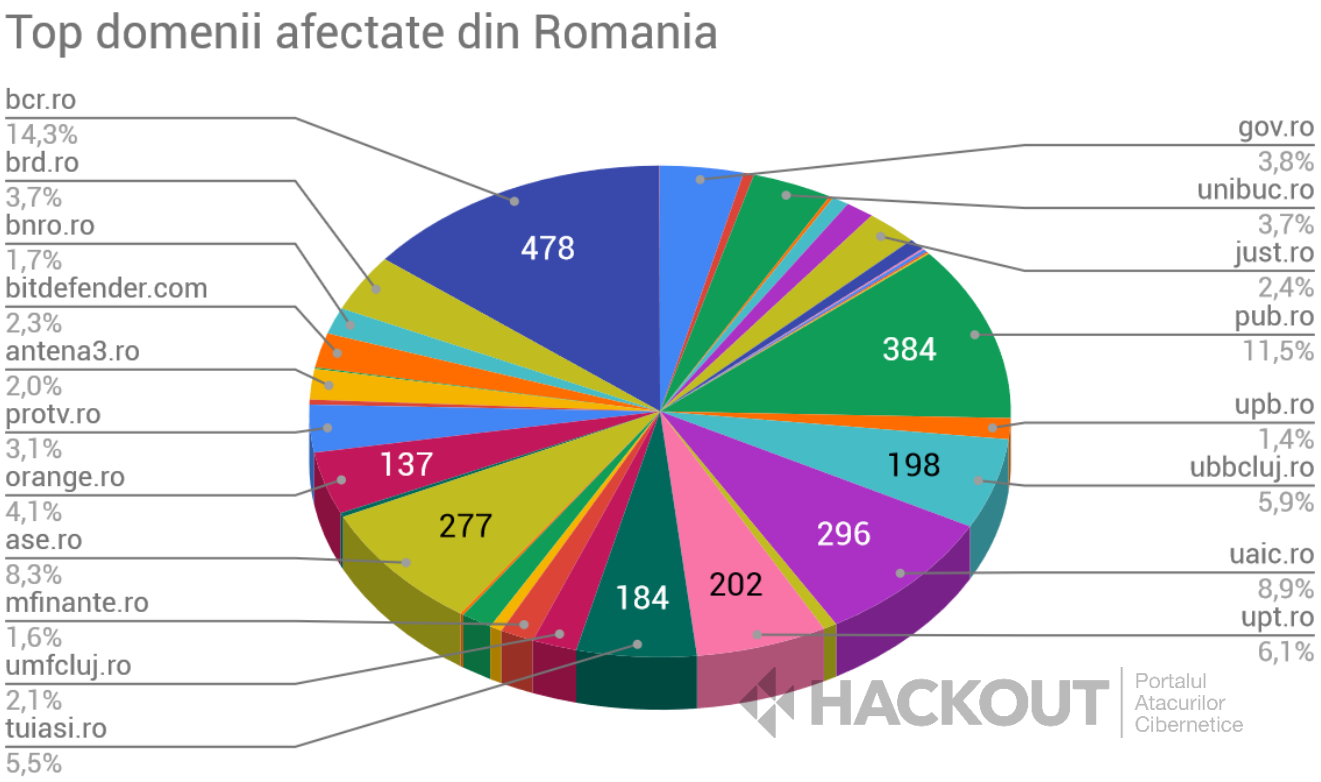
Continuând analiza datelor am început să investigăm fiecare fișier în parte și să le clasificăm în funcție de domeniile mailurilor.

Yahoo - 31% Gmail - 42% Mail.ru + rusia 18% Altele 9%



Faptul că datele sunt împărțite pe EU, SUA, RU și denumirile fișierelor mai sus menționate ne indică faptul că deși atacurile au fost dinspre zona estică, nu toate au fost țintite asupra UE și SUA, dar și spre Rusia.

Am început mai departe o analiză amănunțită și am filtrat toate mailurile ce aparțin instituțiilor publice și a funcționarilor publici din România.



Acestea sunt în total 3,334 de conturi de e-mail și parolele aferente acestora stocate în clar-text.

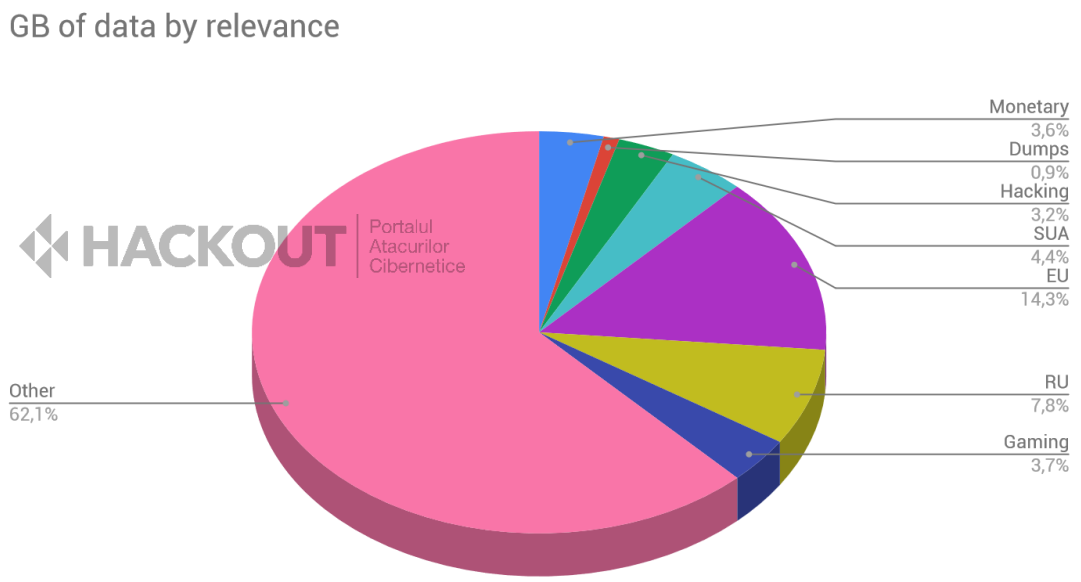
5.Collection#2

Conținutul

Colecția a doua conține un numar de 32 de foldere, care arhivate au dimensiunea de **206GB** si dezarhivate **370GB** (11,969 fisiere). Acestea sunt împărțite în funcție de relevanță datelor, exact ca în prima Colectie (#1).

- ANTIPUBLIC #1
- ANTIPUBLIC #1_MYRQ ANTIPUBLIC
- AP MYR & ZABUGOR #2
- AP MYR & ZABUGOR #2_EU + RUSSIAN ANTIPUBLIC
- Collection #2_New combo cloud_Database Collection_Dump расшифрованные
- Collection #2_New combo cloud_Database Collection_Gaming Databases
- Collection #2_New combo cloud_Domain Specific Collection
- Collection #2_New combo cloud_Gaming Collection
- Collection #2_New combo cloud_Gaming Collection_Gaming Splits
- Collection #2_New combo cloud_General Splits Collection
- Collection #2_New combo cloud_Hacking Related Collection
- Collection #2_New combo cloud_Mail Access Collection
- Collection #2_New combo cloud_Money Related Collection
- Collection #2_New combo cloud_Number Collection
- Collection #2_New combo cloud_Private Collection
- Collection #2_New combo cloud_Region Specific Collection_com
- Collection #2_New combo cloud_Region Specific Collection_edu
- Collection #2_New combo cloud_Region Specific Collection_gov
- Collection #2_New combo cloud_Region Specific Collection_net
- Collection #2_New combo cloud_Region Specific Collection_org
- Collection #2_New combo cloud_Region Specific Collection_Others
- Collection #2_New combo cloud_Unsorted Collection
- Collection #2_New combo cloud_UPDATES_November 4th 2018_EU combo
- Collection #2_New combo cloud_UPDATES_November 4th 2018_Update Dumps
- Collection #2_New combo cloud_UPDATES_November 4th 2018_Update Dumps_Dumps
- Collection #2_New combo cloud_UPDATES_November 7th 2018_Domain Specific Lists
- Collection #2_New combo cloud_UPDATES_November 7th 2018_Region Specific Lists
- Collection #2_New combo cloud_UPDATES_November 9th 2018_Domain Sorted
- Collection #2_New combo cloud_UPDATES_November 9th 2018_Region Sorted
- Collection #2_New combo cloud_UPDATES_Update 08 01 2019
- Collection #2_New combo cloud_VIP Collection
- Collection #2_New combo cloud_VIP Collection_More Lists

Observăm mai departe că cele mai mari date sunt **combo**-urile (notate cu Others în grafic) și conturile de **Europa**.

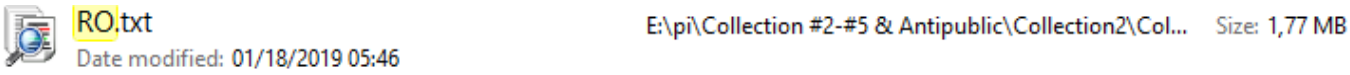


Website-urile din România ce apar în dump-uri sunt urmatoarele: (**cifra din dreapta reprezintă numarul de conturi afectate**)

alimente-geriatrice.ro	586	macheteshop.ro	4212	ktd.ro	5798
transindex.ro	1575	propack-romania.ro	9664	cartestraina.ro	22810
vacantesicalatorii.ro	27780	meteorpress.ro	1645	biocom-international.ro	21482
secpral.ro	18281	ase.ro	4198	linkweb.ro	55982
psihologieonline.ro	5505	mobotix.ro	3204	integrame.ro	31232
my-press.ro	3777	kgb-hosting.ro	218	experimental.ro	23713
legisplus.ro	3554	jobee.ro	2129	sferajuridica.ro	1264
ktd.ro	5798	jobstore.ro	4623	legisplus.ro	3554
experts.ro	177192	garnituri.ro	11220	rnt.ro	14991
irecson.ro	531				

În total, **466,518** de conturi ce provin din site-uri (dump-uri) românești.

Ceea ce ne-a atras atenția după ce am găsit aceste site-uri românești afectate, a fost un fișier intitulat ,,RO.txt”



Acesta conține nu mai mult și nici mai puțin de **55,263** conturi, de la diferite firme și instituții cheie, toate din România.

Blueair.ro	Rds-rcs.ro	Posta-romana.ro	Urgent-curier.ro
Transelectrica.ro	Romtelecom.ro	Tarom.ro	Unicredit.ro
Catmusic.ro	Milenniumbank.ro	Mfinante.ro	Bcr.ro
Tvr.ro	Provident.ro	Ase.ro	Bancpost.ro

În folder apar mai multe țări: PL, RO, RU, UA, UK, USA, ZAB.

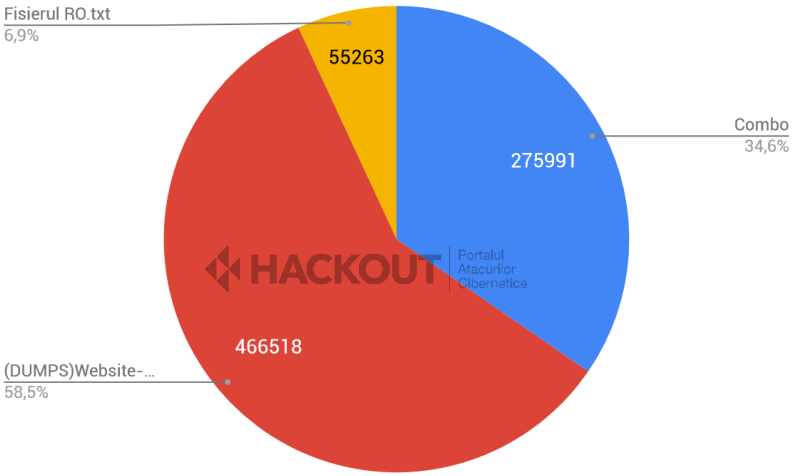
Iar pe lângă acestea, mai avem din fișierele de combo-uri, un numar de **275,991** conturi din România ce figurează în această colecție.

Sursa datelor

Comparând sursa lor, dump-uri vs. combo-uri, observăm în continuare – similar cu Colecția #1 – faptul că majoritatea conturilor compromise nu sunt din site-urile Românești afectate, ci din liste în care sunt puse laolaltă cu multe alte conturi din alte țări provenite cel mai probabil din breșe mai vechi (2008-2017).

Așadar, în Collection#2 avem un total de

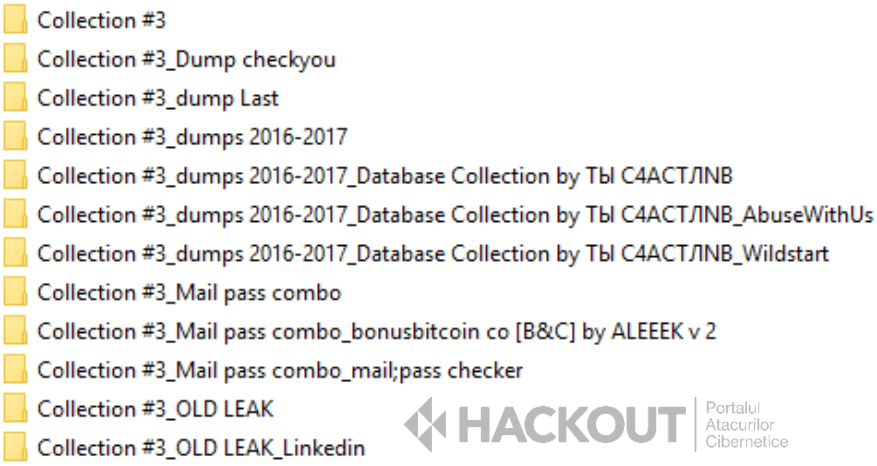
797,772 conturi din România.



6.Collection#3

Conținutul

Colecția a treia conține un număr de **12** de foldere, care arhivate au dimensiunea de **15,9GB** și dezarhivate **44,7GB** (2,096 fisiere). Aceasta este cea mai mică colecție și nu conține date foarte relevante pentru România.



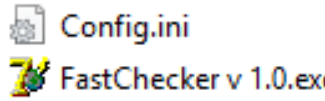
Colecția conține în mare parte câteva leak-uri mai vechi:

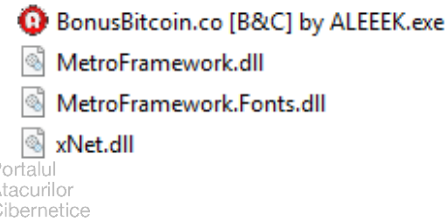
- AbuseWithUs
- LinkedIn
- CheckYou
- Fling
- Last.Fm
- Vk.com
- 000webhost.com

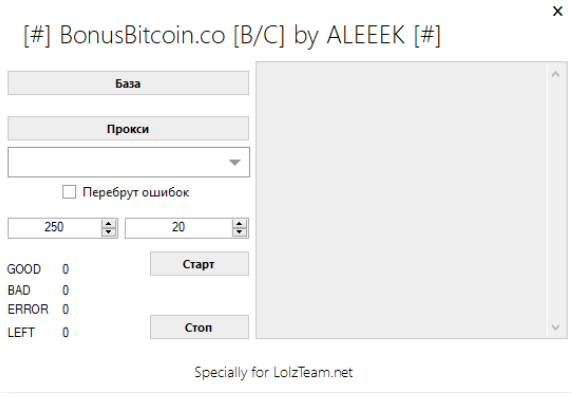
+ altele

Soft-uri incluse

Cel mai interesant lucru din arhiva aceasta, observat la prima vedere, este faptul că sunt incluse două programe software de tip – **account checkers** – programe în care hackerii introduc **combo-list**-uri (e-mailuri și parole în format .txt), iar acestea testează pe diferite site-uri conturile respective.







Exemplificare

Spre exemplu, ei fac rost de o bază de date ce conține conturi de facebook si testează respectiva bază de date cu ajutorul unui checker pe restul rețelelor sociale, site-urilor bancare, paypal etc.

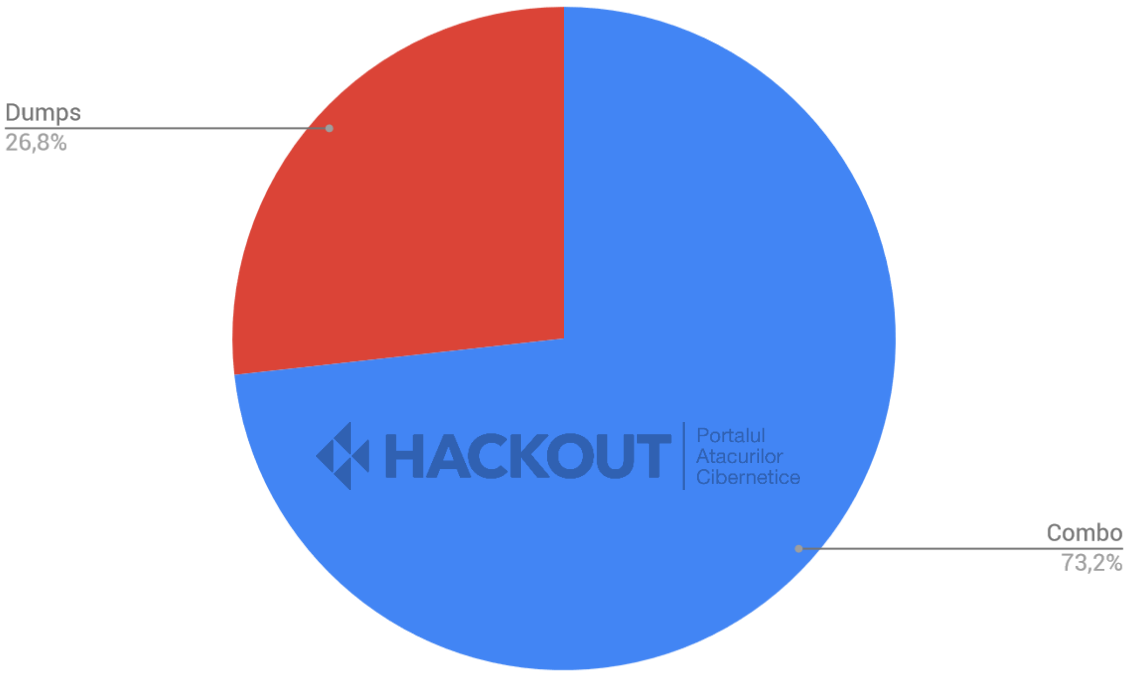
În cazurile de mai sus, unul dintre ele este pentru platforme sociale, iar al doilea pentru un site de Bitcoin trading.

Tocmai de aceea este recomandat să folosiți parole diferite pentru toate aplicațiile.

Website-uri românești compromise în această arhivă sunt doar 3:

- Propack-romania.ro (14,334)
- Caro.ro (22,437)
- Anuntulmagic.ro (139,011)

În total dump-urile contin **175,782** de conturi din România, la acestea adaugăm încă **289,132** conturi găsite de noi în restul de Combo-uri.

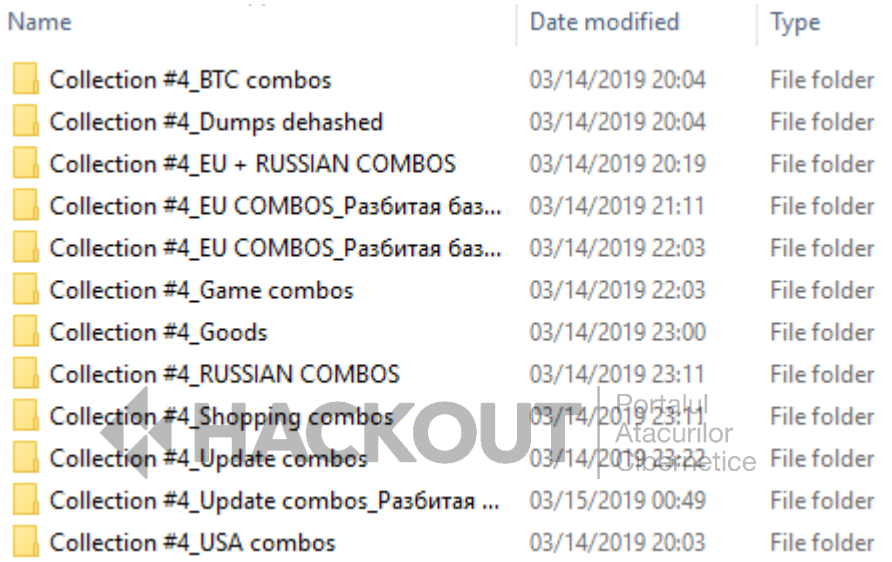


Așadar, în total, în Collection#3 avem un număr de **464,914** conturi din România.

7.Collection#4

Conținutul

Colecția a patra conține un numar de **12** de foldere, care arhivate au dimensiunea de **76,4GB** și dezarhivate **178GB** (39,937 fișiere). Aceasta nu conține date foarte relevante pentru România.



Name	Date modified	Type
Collection #4_BTC combos	03/14/2019 20:04	File folder
Collection #4_Dumps dehashed	03/14/2019 20:04	File folder
Collection #4_EU + RUSSIAN COMBOS	03/14/2019 20:19	File folder
Collection #4_EU COMBOS_Разбитая баз...	03/14/2019 21:11	File folder
Collection #4_EU COMBOS_Разбитая баз...	03/14/2019 22:03	File folder
Collection #4_Game combos	03/14/2019 22:03	File folder
Collection #4_Goods	03/14/2019 23:00	File folder
Collection #4_RUSSIAN COMBOS	03/14/2019 23:11	File folder
Collection #4_Shopping combos	03/14/2019 23:11	File folder
Collection #4_Update combos	03/14/2019 23:22	File folder
Collection #4_Update combos_Разбитая ...	03/15/2019 00:49	File folder
Collection #4_USA combos	03/14/2019 20:03	File folder

Din câte putem observa, această colecție conține în mare parte Combo-uri de Europa, Rusia, Bitcoin, Jocuri și SUA.

Cel mai important fișier din toată colecția îl reprezintă folderul „**WALLMART**” în care sunt aproximativ ~**25GB** de date personale a clienților lanțului de magazine cu același nume.

Din România, figurează doar **260,114** conturi. Acestea nu sunt foarte relevante deoarce echipa noastra a analizat o parte dintre aceste date și am constatat că ele au fost colectate între anii **2011-2015**, iar leak-urile din care fac parte aceste date sunt leak-uri deja raportate.

Așadar, toate parolele sunt deja schimbate de către utilizatorii respectivi (sau cel puțin ar trebui să fie).

Cele mai afectate domenii din România ce figurează în această colecție sunt:

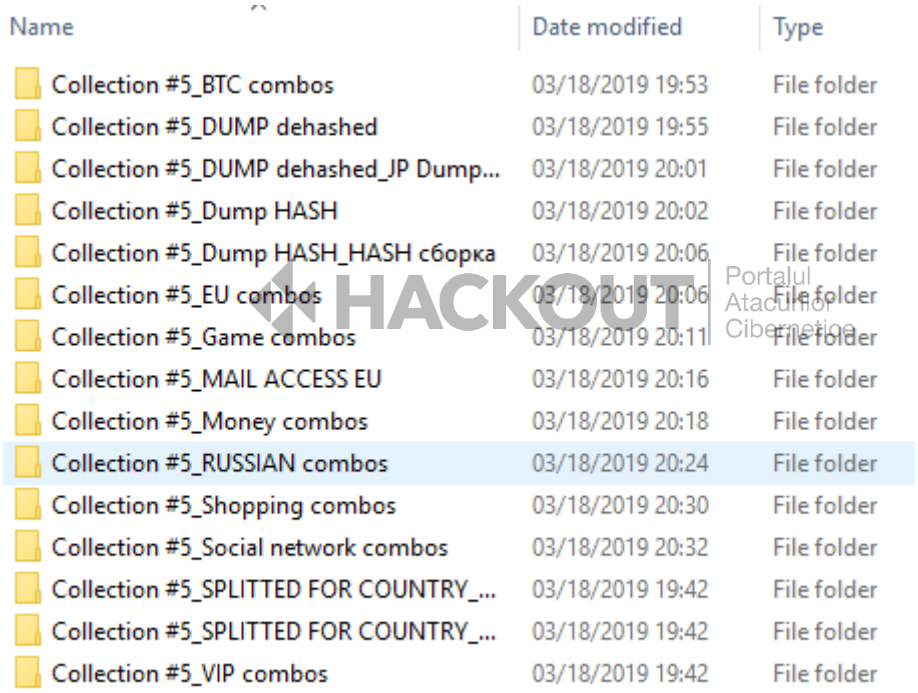
- Upc.ro
- Yahoo.ro
- K.ro
- Brd.ro
- Rdslink.ro
- Atestatehtml.ro
- Gov.ro
- Bnr.ro
- Insse.ro
- Pub.ro
- Mfinante.ro

Recomandăm totuși să vă verificați e-mailurile în secțiunea de verificare: https://hackout.ro .

8.Collection#5

Conținutul

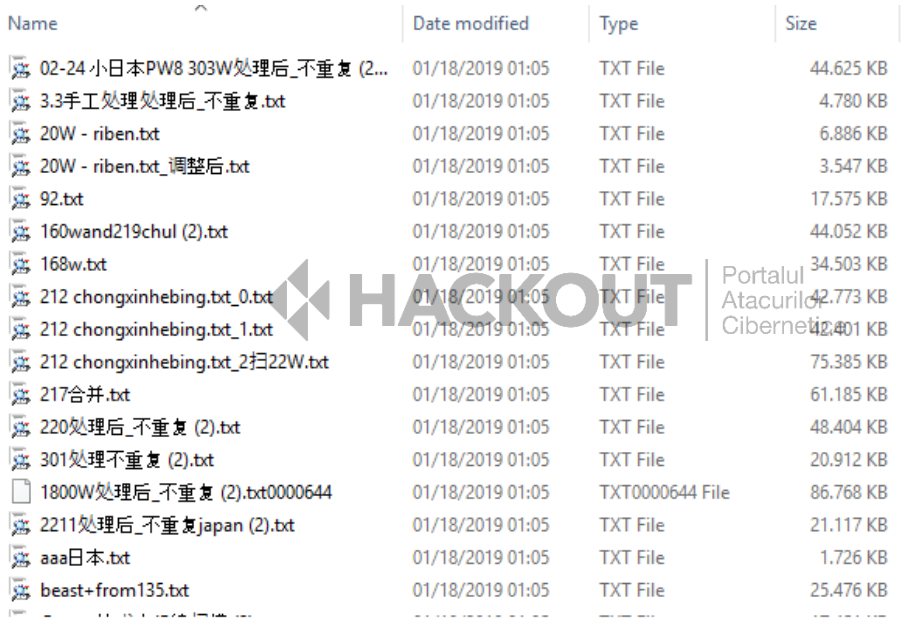
Colecția a cincea conține un număr de **15** de foldere, care arhivate au dimensiunea de **17,7GB** și dezarhivate **40,5GB** (16,026 fișiere).



Name	Date modified	Type
Collection #5_BTC combos	03/18/2019 19:53	File folder
Collection #5_DUMP dehashed	03/18/2019 19:55	File folder
Collection #5_DUMP dehashed_JP Dump...	03/18/2019 20:01	File folder
Collection #5_Dump HASH	03/18/2019 20:02	File folder
Collection #5_Dump HASH_HASH сборка	03/18/2019 20:06	File folder
Collection #5_EU combos	03/18/2019 20:06	File folder
Collection #5_Game combos	03/18/2019 20:11	File folder
Collection #5_MAIL ACCESS EU	03/18/2019 20:16	File folder
Collection #5_Money combos	03/18/2019 20:18	File folder
Collection #5_RUSSIAN combos	03/18/2019 20:24	File folder
Collection #5_Shopping combos	03/18/2019 20:30	File folder
Collection #5_Social network combos	03/18/2019 20:32	File folder
Collection #5_SPLITTED FOR COUNTRY_...	03/18/2019 19:42	File folder
Collection #5_SPLITTED FOR COUNTRY_...	03/18/2019 19:42	File folder
Collection #5_VIP combos	03/18/2019 19:42	File folder

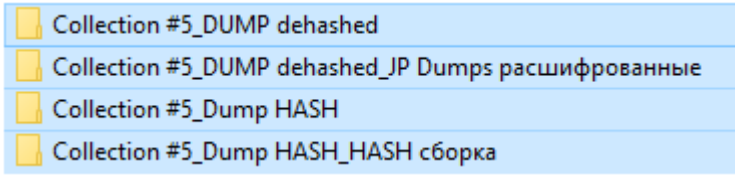
,,JP" – Japan

Colecția a V-a este prima și singura dintre cele 5 colecții ce conține un folder întreg de conturi din Japonia.



Name	Date modified	Type	Size
02-24 小日本PW8 303W处理后_不重复 (2...	01/18/2019 01:05	TXT File	44.625 KB
3.3手工处理处理后_不重复.txt	01/18/2019 01:05	TXT File	4.780 KB
20W - riben.txt	01/18/2019 01:05	TXT File	6.886 KB
20W - riben.txt_调整后.txt	01/18/2019 01:05	TXT File	3.547 KB
92.txt	01/18/2019 01:05	TXT File	17.575 KB
160wand219chul (2).txt	01/18/2019 01:05	TXT File	44.052 KB
168w.txt	01/18/2019 01:05	TXT File	34.503 KB
212 chongxinhebing.txt_0.txt	01/18/2019 01:05	TXT File	42.773 KB
212 chongxinhebing.txt_1.txt	01/18/2019 01:05	TXT File	42.401 KB
212 chongxinhebing.txt_2扫22W.txt	01/18/2019 01:05	TXT File	75.385 KB
217合并.txt	01/18/2019 01:05	TXT File	61.185 KB
220处理后_不重复 (2).txt	01/18/2019 01:05	TXT File	48.404 KB
301处理不重复 (2).txt	01/18/2019 01:05	TXT File	20.912 KB
1800W处理后_不重复 (2).txt0000644	01/18/2019 01:05	TXT0000644 File	86.768 KB
2211处理后_不重复japan (2).txt	01/18/2019 01:05	TXT File	21.117 KB
aaa日本.txt	01/18/2019 01:05	TXT File	1.726 KB
beast+from135.txt	01/18/2019 01:05	TXT File	25.476 KB

4 din cele 15 foldere sunt reprezentate de DUMP-uri



Website-uri din **România** prezente în aceste dump-uri sunt urmatoarele:

Revizieshop.ro	Deviz.ro	Piatadeporumbei.ro	Jobstore.ro
Oilshop.ro	Barcacuda.com.ro	Mondo-romania.ro	Fundatiasnagov.ro
Megapreturi.ro	Airosft.ro	Mobotix.ro	Compass.ro
Ktd.ro	Amfcluj.ro	Linkweb.ro	Asociatiabrokerilor.ro
Informatiaprahive.ro	Zwcad.ro	Elth.pub.ro	
Favisan.ro			

În total acestea reprezinta **491,476** de conturi – doar din dump-uri; acestora le adăugăm încă **1,002,331** de conturi din România ce se află în restul de fișiere – combo-uri.

În total, această arhivă are aproape **1,5 milioane** de conturi românești.

9.Concluzii

Pe parcursul analizei celor 5 colecții am observat faptul că unele dump-uri ale site-urilor românești se repetă în toate cele 5 colecții (ex: ktd.ro, mobotix.ro etc). Cel mai probabil acestea sunt cele mai căutate și cele mai vândute pe DarkWeb, dar și pe forumurile publice de pe internet.

Însumând toate cele 5 colecții

Collection**#1**	**2,316,011**
Collection**#2**	**797,772**
Collection**#3**	**464,914**
Collection**#4**	**260,114**
Collection**#5**	**1,493,807**

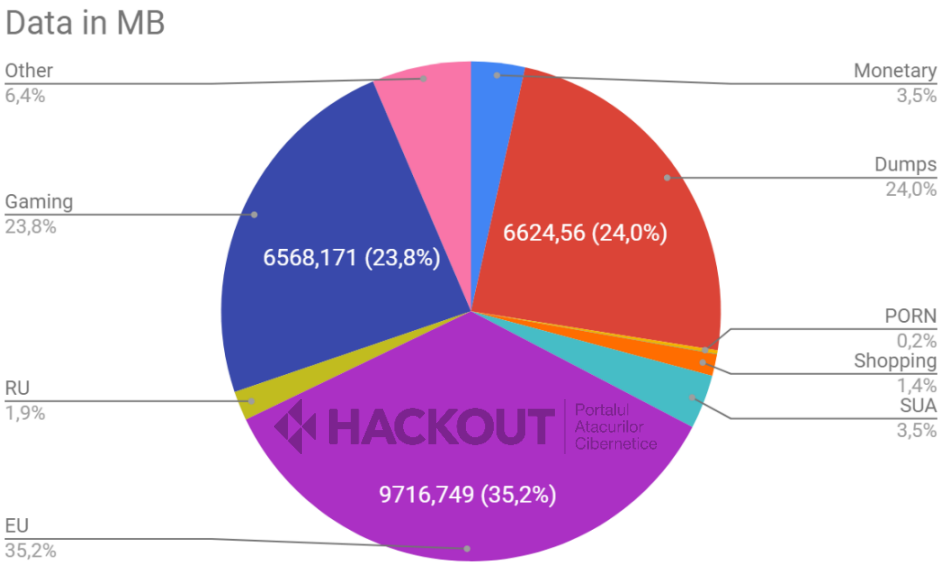
Total: **5,332,618** de conturi românești

Așadar, acest leak este unul dintre cele mai mari leak-uri din istorie la momentul actual, atât la nivel global cât și la nivel național. Totalul de 5,3 milioane reprezintă o cifră destul de inexactă deoarece multe conturi se repetă de-alungul colecțiilor. Așadar, prin analiză statistică și un algoritm de unique key indexing ajungem la un număr de 1,7 milioane de conturi românești unice.

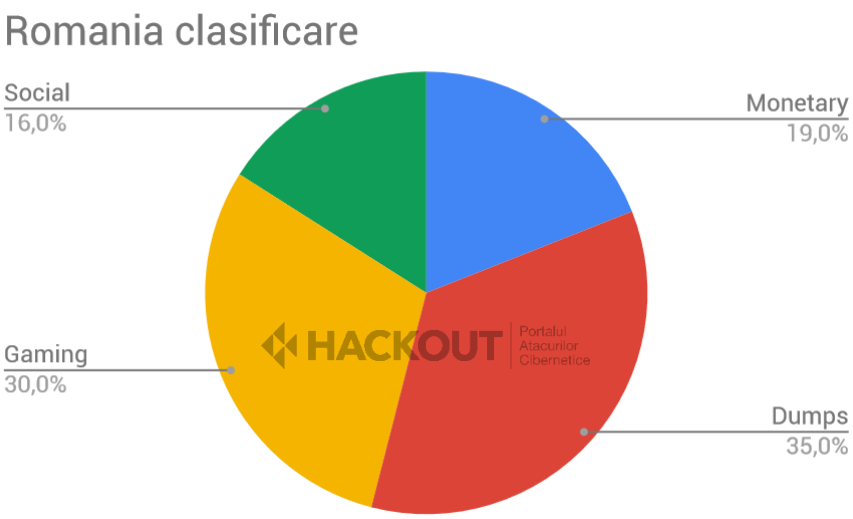
Acestea sunt reprezentate în mare parte de mail-uri, parole, adrese, numere de telefon și alte date personale, iar majoritatea sunt marcate ca relevante pentru domeniile financiare și jocuri, acestea fiind probabil cele mai frecvente surse ale naturii lor.

Graficul pe domenii de interes prezentat în capitolul Collection#1 este cel mai relevant, deoarece cele mai noi date și cele mai multe sunt cele din Collection#1.

Așadar, avem următoarea statistică:



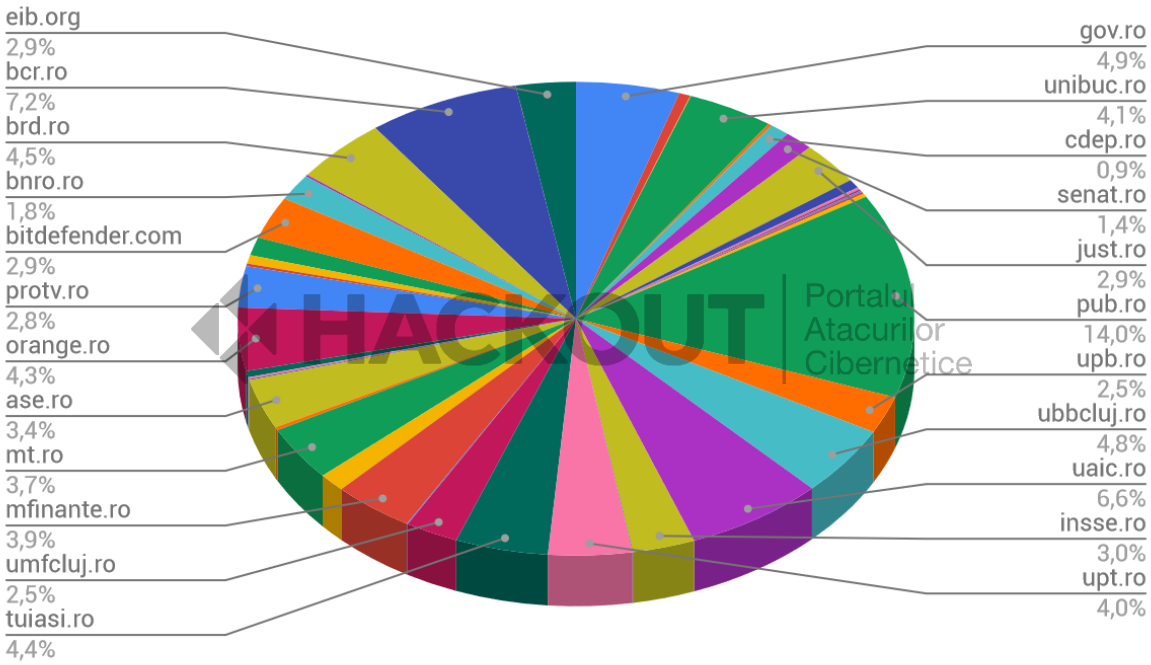
În cazul **României**, situația este relativ similară



Pe lângă aceste date, echipa noastră a realizat un studiu complet asupra unora dintre cele mai relevante domenii regăsite prin acest leak.

Următorul tabel însumează conturile ce aparțin domeniilor românești sau domeniilor foarte relevante. Aceste valori sunt aproximative.

Domeniu	Numar de conturi compromise	Domeniu	Numar de conturi compromise	Domeniu	Numar de conturi compromise
gov.ro	823	upb.ro	423	vodafone.ro	72
politiaromana.ro	91	ubbcluj.ro	796	orange.ro	717
anaf.ro	5	uaic.ro	1101	protv.ro	468
unibuc.ro	687	insse.ro	496	digi24.ro	30
anpc.ro	28	patriarhia.ro	4	antena3.ro	97
cdep.ro	156	upt.ro	666	huawei.com	14024
senat.ro	231	tuiasi.ro	738	microsoft.com	205330
just.ro	486	umfcluj.ro	421	bitdefender.ro	207
mpublic.ro	101	diicot.ro	8	bitdefender.com	483
juridice.ro	23	mfinante.ro	644	bnro.ro	299
inm-lex.ro	4	mae.ro	211	Alte banci	20
europa.eu	145442	mt.ro	621	brd.ro	751
europal.europa.eu	799	distributie-energie.ro	36	bcr.ro	1207
pna.ro	15	energie.ro	8	bt.ro	18
sri.ro	17	e-distributie.com	3	eib.org	475
presidency.ro	24	ase.ro	566	ec.europa.eu	4204
psd.ro	39	umfcd.ro	11	curia.europa.eu	44994
pub.ro	2331	rcs-rds.ro	22		



Pe de altă parte, am corelat atacul cibernetic raportat de mai mulți europarlamentari în luna februarie a acestui an, raportat chiar de europarlamentarul **Ioan Mircea Pascu** (https://www.dcnews.ro/mircea-pascu-sunt-victima-unui-atac_636795.html)

Cel mai probabil, acesta a primit notificare de la serviciul de monitorizare de pe HaveIBeenPwned.

Analizând și cautând domeniile foarte afectate și cele care au fost vehiculate pe forumuri, am gasit urmatoarele cifre.

europal.europa.eu	329
europa.eu	4069
microsoft.com	44994
huawei.com	3753

ACESTE DATE SUNT CRITICE DEOARECE POT PERMITE ACCESUL ÎN PLATFORME GUVERNAMENTALE / PUBLICE