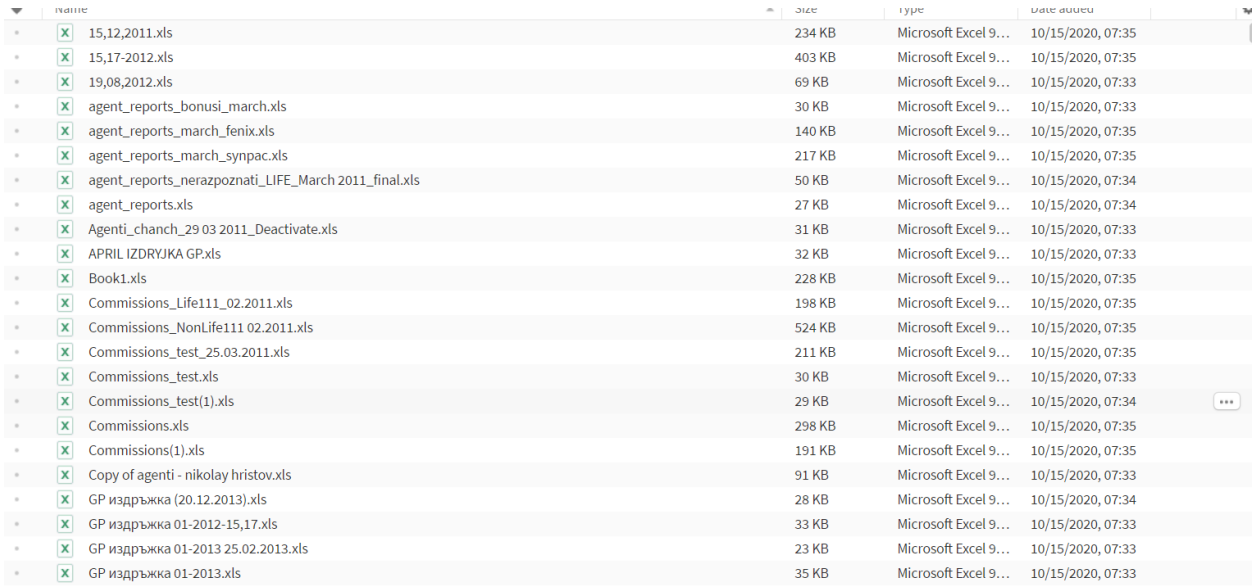
00. Exposing Bulgaria's Kyulev Data Leak Hacker - An OSINT Analysis



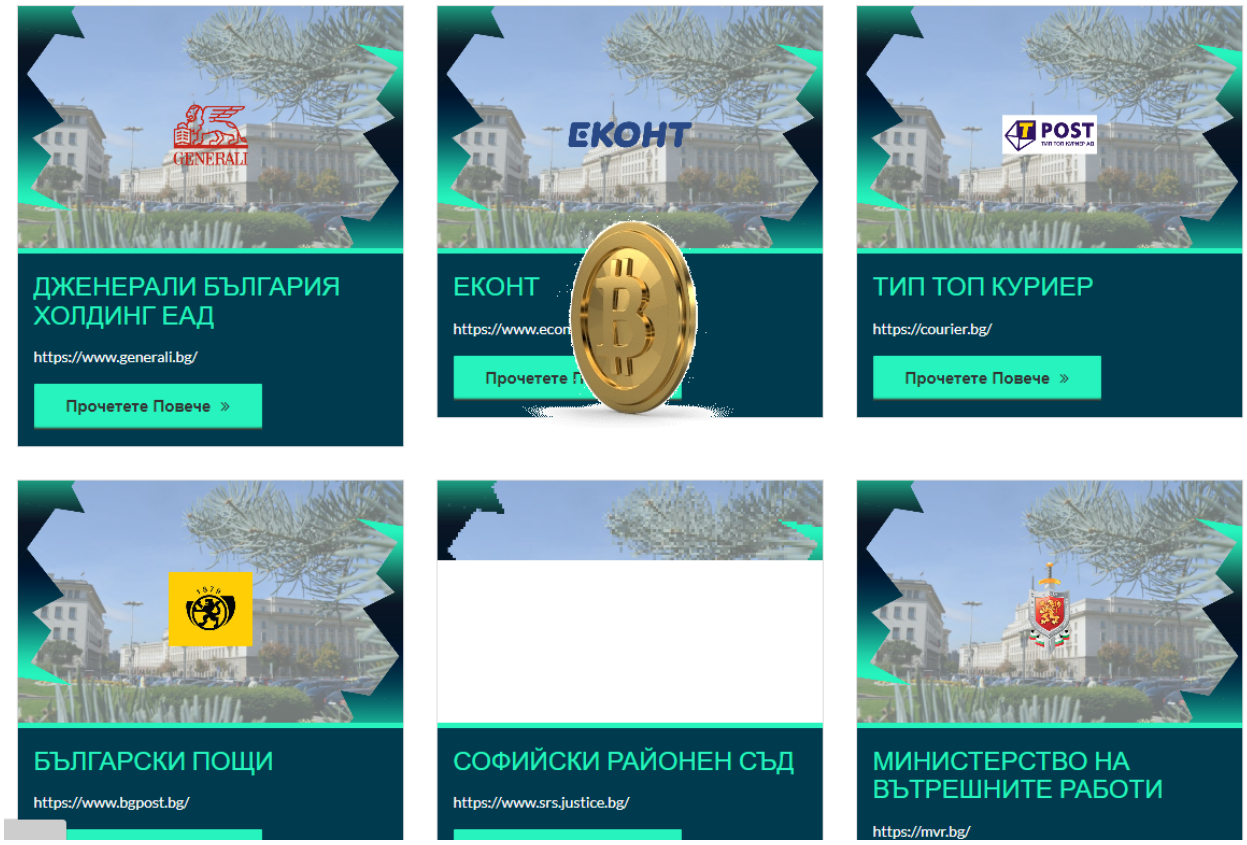
Name	Size	Type	Date added
15,12,2011.xls	234 KB	Microsoft Excel 9…	10/15/2020, 07:35
15,17-2012.xls	403 KB	Microsoft Excel 9…	10/15/2020, 07:35
19,08,2012.xls	69 KB	Microsoft Excel 9…	10/15/2020, 07:33
agent_reports_bonusi_march.xls	30 KB	Microsoft Excel 9…	10/15/2020, 07:33
agent_reports_march_fenix.xls	140 KB	Microsoft Excel 9…	10/15/2020, 07:35
agent_reports_march_synpac.xls	217 KB	Microsoft Excel 9…	10/15/2020, 07:35
agent_reports_nerazpoznati_LIFE_March 2011_final.xls	50 KB	Microsoft Excel 9…	10/15/2020, 07:34
agent_reports.xls	27 KB	Microsoft Excel 9…	10/15/2020, 07:34
Agenti_chanch_29 03 2011_Deactivate.xls	31 KB	Microsoft Excel 9…	10/15/2020, 07:33
APRIL IZDRYJKA GP.xls	32 KB	Microsoft Excel 9…	10/15/2020, 07:33
Book1.xls	228 KB	Microsoft Excel 9…	10/15/2020, 07:35
Commissions_Life111_02.2011.xls	198 KB	Microsoft Excel 9…	10/15/2020, 07:35
Commissions_NonLife111 02.2011.xls	524 KB	Microsoft Excel 9…	10/15/2020, 07:35
Commissions_test_25.03.2011.xls	211 KB	Microsoft Excel 9…	10/15/2020, 07:35
Commissions_test.xls	30 KB	Microsoft Excel 9…	10/15/2020, 07:33
Commissions_test(1).xls	29 KB	Microsoft Excel 9…	10/15/2020, 07:34
Commissions.xls	298 KB	Microsoft Excel 9…	10/15/2020, 07:35
Commissions(1).xls	191 KB	Microsoft Excel 9…	10/15/2020, 07:35
Copy of agenti - nikolay hristov.xls	91 KB	Microsoft Excel 9…	10/15/2020, 07:33
GP издръжка (20.12.2013).xls	28 KB	Microsoft Excel 9…	10/15/2020, 07:34
GP издръжка 01-2012-15,17.xls	33 KB	Microsoft Excel 9…	10/15/2020, 07:33
GP издръжка 01-2013 25.02.2013.xls	23 KB	Microsoft Excel 9…	10/15/2020, 07:33
GP издръжка 01-2013.xls	35 KB	Microsoft Excel 9…	10/15/2020, 07:33

We've decided to take a deeper look inside the Internet-connected infrastructure of a well known Bulgarian data leaker who's known to have compromised several high-profile targets in Bulgaria and is currently offering access to the compromised databases.

In this analysis we'll take a deeper look inside the Internet-connected infrastructure of Bulgaria's Kyulev data leak hacker for the purpose of assisting international Law Enforcement including the security industry in terms of monitoring and tracking down the cybercriminal's activities.

Sample domains known to have been involved in the campaign include:

hxxp://reket2021.to
hxxp://dadsagency.cc
hxxp://dadsagency.pw
hxxp://dadsagency.org
hxxp://dadsagency.ws
hxxp://dadsagency.xyz
hxxp://dadsagency.to



Sample personally identifiable email address accounts known to have been involved in the campaign include:

dadsagency@tutanota.com
e.kyulev@protonmail.com

Sample responding IPs known to have been involved in the campaign include:

104.21.27.11
172.67.146.108
104.21.41.181
104.21.83.44
172.64.192.34
104.21.3.46
104.21.47.22
172.67.149.89
216.120.146.201
172.67.168.238

199.59.243.200
172.67.130.60
104.21.29.102
172.67.175.244
64.70.19.34
172.67.143.137
104.21.81.185
104.21.41.58
64.70.19.203
172.67.163.98
91.195.240.117

We'll continue monitoring the campaign and will post updates as soon as new developments take place.