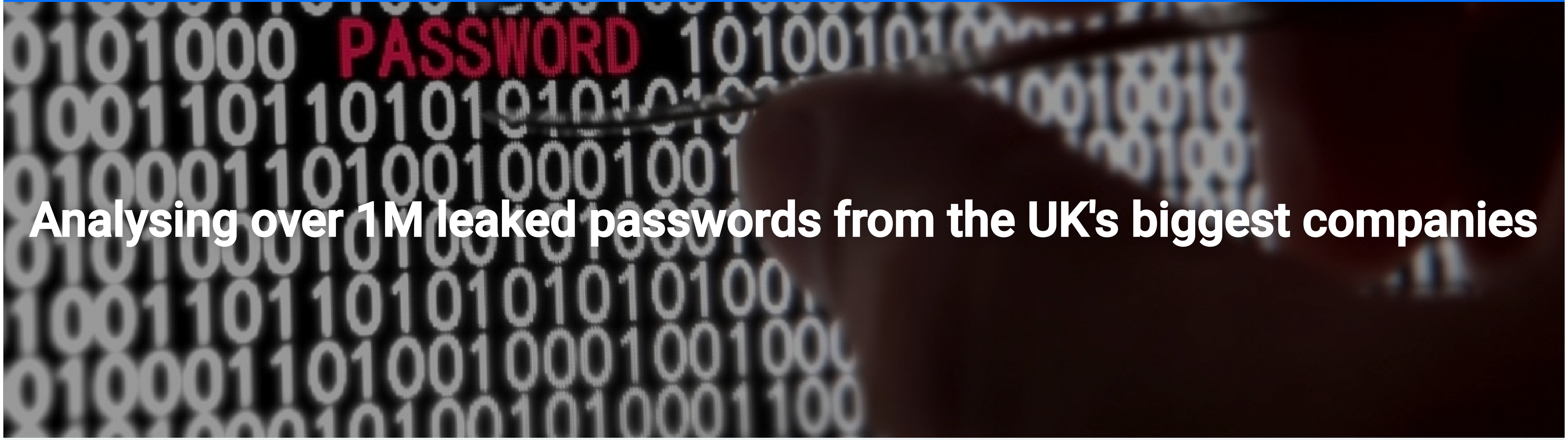


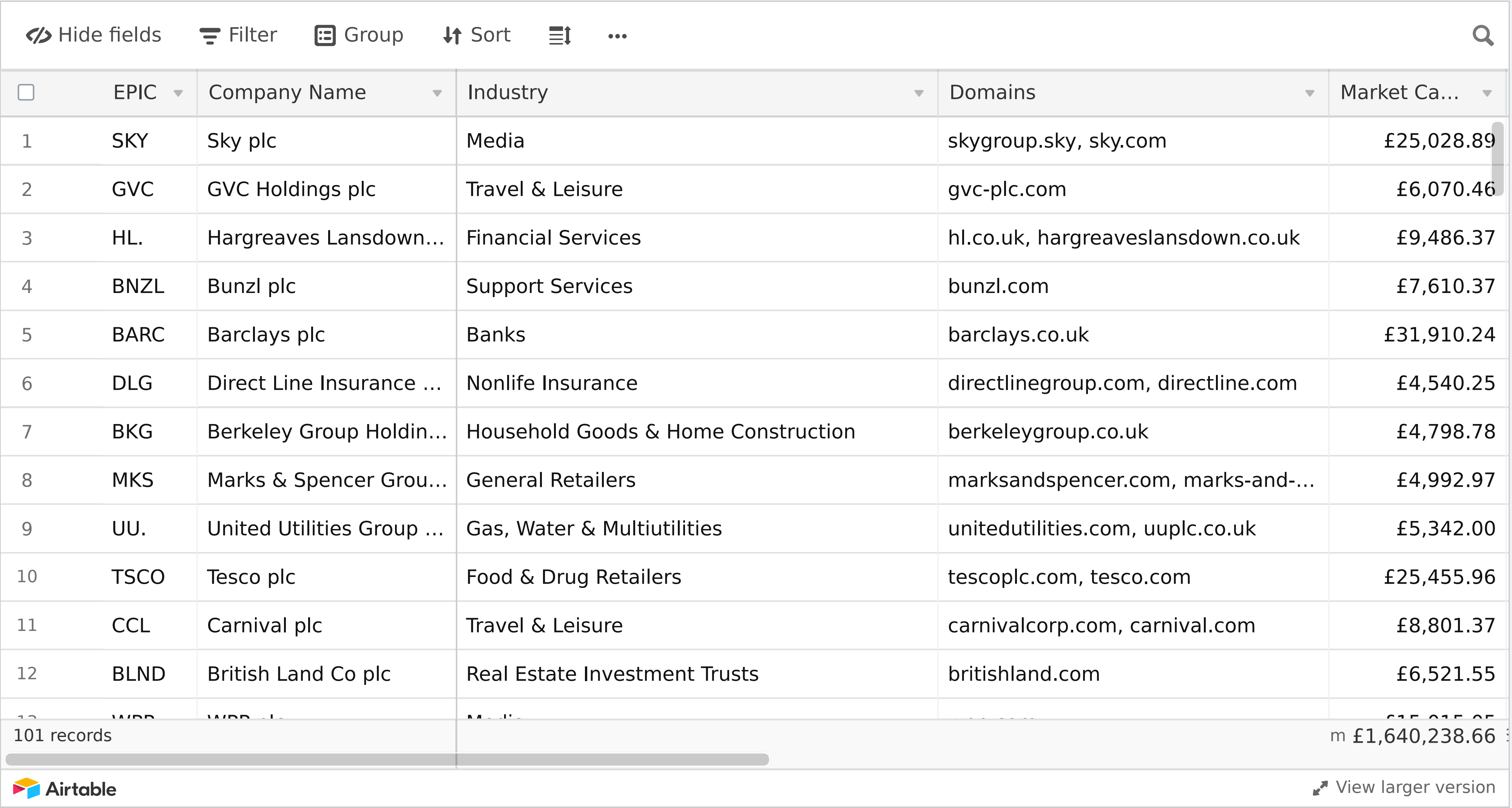
Analysing over 1M leaked passwords from the UK's biggest companies

Thursday, 21st May 2020

Tweet Share

How do some of the UK's biggest companies fair when it comes to passwords? Does their large size — and presumably their large cyber security budgets — mean better password hygiene by their employees? Let's dive straight in and take a look at public data breaches containing FTSE100 companies:

Cut to chase? Financial services firm Hargreaves Lansdown fair the worst whilst supermarket Morrisons and Unilever come out on top in terms of their password hygiene. The Financial Services and Pharmaceuticals & Biotechnology sectors rank the worst and best respectively.



	EPIC	Company Name	Industry	Domains	Market Ca...
1	SKY	Sky plc	Media	skygroup.sky, sky.com	£25,028.89
2	GVC	GVC Holdings plc	Travel & Leisure	gvc-plc.com	£6,070.46
3	HL.	Hargreaves Lansdown...	Financial Services	hl.co.uk, hargreaveslansdown.co.uk	£9,486.37
4	BNZL	Bunzl plc	Support Services	bunzl.com	£7,610.37
5	BARC	Barclays plc	Banks	barclays.co.uk	£31,910.24
6	DLG	Direct Line Insurance ...	Nonlife Insurance	directlinegroup.com, directline.com	£4,540.25
7	BKG	Berkeley Group Holdin...	Household Goods & Home Construction	berkeleygroup.co.uk	£4,798.78
8	MKS	Marks & Spencer Grou...	General Retailers	marksandspencer.com, marks-and-...	£4,992.97
9	UU.	United Utilities Group ...	Gas, Water & Multiutilities	unitedutilities.com, uuplc.co.uk	£5,342.00
10	TSCO	Tesco plc	Food & Drug Retailers	tescoplc.com, tesco.com	£25,455.96
11	CCL	Carnival plc	Travel & Leisure	carnivalcorp.com, carnival.com	£8,801.37
12	BLND	British Land Co plc	Real Estate Investment Trusts	britishland.com	£6,521.55
13	WPP	WPP plc	Media	wpp.com	£15,015.05

101 records

m £1,640,238.66

The data is sorted by two averaged metrics: the password score between 0 - 4 and the number of guesses needed to crack the password *(log)*. The lower the scores the more the password is deemed insecure and easier to guess. For example, a password score of 2.0 means it's somewhat guessable and has protection from unthrottled online attacks *(guesses < 10^8)*.

You'll note the first two companies, Sky and GVC Holdings, have empty score and guesses columns. Sky provide their customers with a @sky.com e-mail address so there's no surprise that we find them at the top of the list in terms of the number of exposed credentials at a whopping 694,560. Because of this we will ignore them for the purposes of this article.

GVC Holdings do not appear in **any** breach lists and Ashtead Group have just 1 leaked password which is very surprising given they have 28,000 and 15,809 employees respectively. I can only imagine the listed company and it's associated domains are not the main operating company. GVC's latest annual report places 'DATA BREACH AND CYBER SECURITY' as their #1 principal risk and state *"The Group dedicates significant resources to ensure security arrangements and systems are up to date to cope with emerging threats"*. Or perhaps they've just out right banned employees creating online accounts with their work e-mails. Which is probably a good idea especially as 71 of the FTSE100 appear in adult dating breach lists - whoops 😬!

Let's dive deeper in to the data and take a look at the top 10 passwords:

```
(count  password)
        1.   10770  123456
        2.    5570  password
```

```
3.     3490  linkedin
4.     2120  12345
5.     1960  liverpool
6.     1690  vodafone
7.     1440  welcome1
8.     1430  password1
9.     1180  chelsea
10.    1140  sunshine
```

Nothing overly exciting and what we would expect to find from any random sample of passwords. Password #6 "*vodafone*" caught my eye as Vodafone ranks fairly well at 82nd on the FTSE100 list with 25,402 leaked passwords and only a mere 2% of them were "*vodafone*" suggesting it is more customers using this as a password and not Vodafone employees. Further down on the list at #19 we see the password "*Unilever123*" largely for Unilever accounts and who rank the highest on the FTSE100 list in terms of password hygiene.

The curious case of 3sYqo15hiL

At #21 we see the password "3sYqo15hiL" which is not typically a common password and perhaps surprisingly appears at around position 13,000 from a random sample. The password is only attributed to @sc.com (Standard Chartered) accounts within our FTSE100 data set. Searching more broadly reveals 8,094 more results and we see that the majority of these passwords were from the Exploit.in compilation leak with a few instances from the Twitter and Yahoo leaks. *Most* of the e-mail addresses associated with this password are seemingly randomly generated:

```
 (email : password)
[...]
ydaf1h9@hotmail.com : 3sYqo15hiL
bvts8d2@gmail.com   : 3sYqo15hiL
ezwr8n0@yahoo.com   : 3syqo15hil
nuxy9u9@sc.com      : 3sYqo15hiL
ohuy4l1@sc.com      : 3sYqo15hiL
[...]
```

You can see the e-mail format is consistently *[4alpha][1number][1alpha][1number]@*. There are a few instances of genuine looking e-mails, for example; rachel.thomson24@gmail.com, sharonmdoyle@yahoo.com, jeff.timmerman@hotmail.com, but it's only around a 92% random / 8% genuine split. I can only think of two reasons why the same password would be used across so many different accounts: the data sets contain false purposely inserted information or this is a systematic bot network.

I can confidently rule out the first theory for three reasons:

1. The same e-mail format pattern and passwords are seen across multiple data sets from different sources; and

2. Using SMTP verification (essentially 'pinging' an e-mail mailbox) I could verify that many of these accounts still exist and were accepting mail; and
3. By using various OSINT techniques I was able to uncover matching social media profiles behind the accounts.

For example, the e-mail address euncieservices@gmail.com appears in 6 seperate breach lists; Bukalapak, "Collection #1", Exploit.in, Go Games, Intelimost, and Programming Forums and was/is seemingly associated with fraudulent activity. It is listed as being linked to the domain name skoronline.org in this Court order filing for selling counterfeit Adidas goods. There are many other instances of these e-mail addresses being 'called out' on forums for spam reasons.

So the most likely explanation is sort of spam bot network. Searching more broadly, here's a breakdown of the top 10 providers used to register these accounts:

```
    (count  password)
             1.   5523  hotmail.com
             2.   1179  yahoo.com
             3.    308  gmail.com
             4.    160  sc.com
             4.    156  yahoo.co.uk
             5.    156  mail.ru
             6.    156  interia.pl
             7.     69  aol.com
```

All free e-mail providers. But what about our @sc.com (Standard Chartered) accounts? Why would one of the UK's biggest financial firms be involved in a spam network? Unlike Sky, users can't registered a Standard Chartered e-mail address. Were they compromised at some point...? After some digging the answer is pretty simple. The sc.com domain was owned by a company called SuperConnect up until early 2009 and users *could* then create a @sc.com e-mail account.

A glimmer of hope?

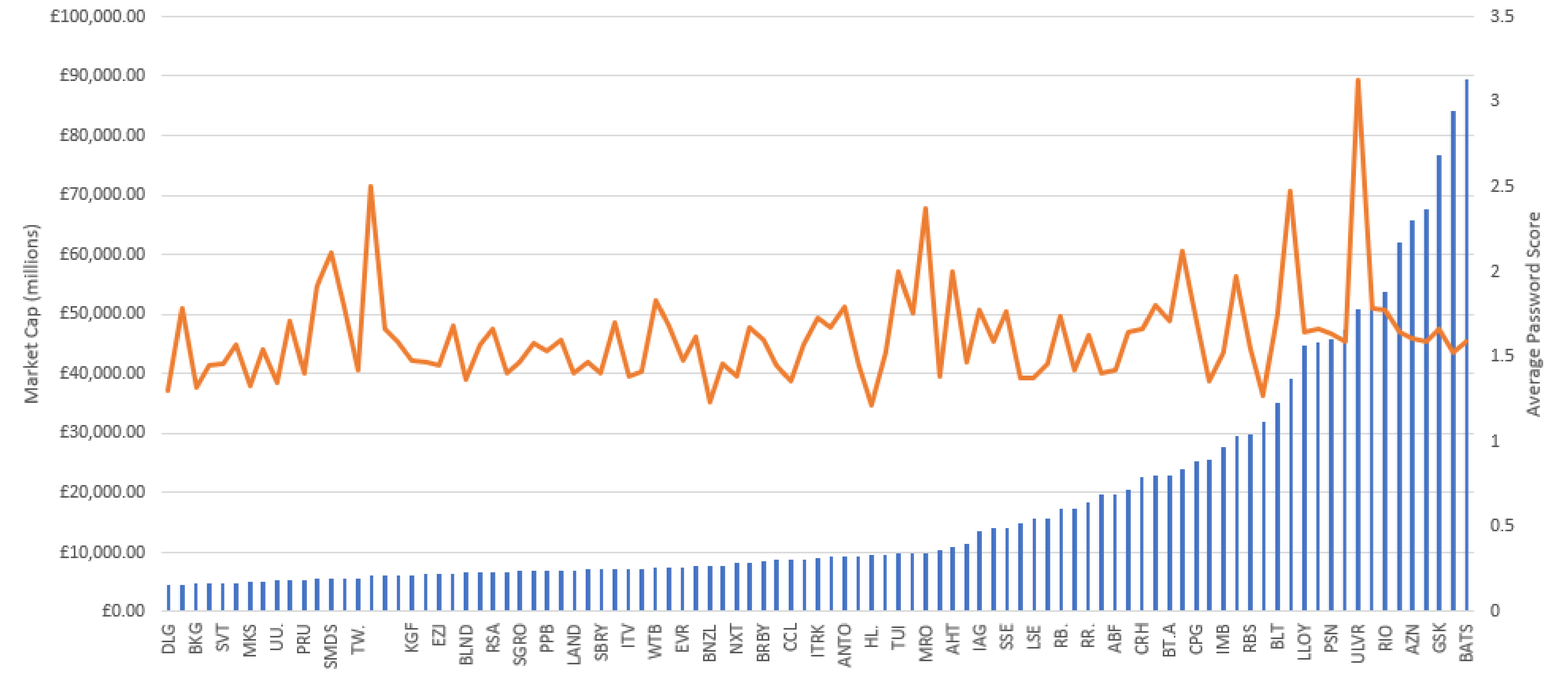
Back to our FTSE100 data set. Why do we see 3i Group with 555 exposed credentials but only 281 employees - more than 3x the exposure in % terms than any other company. Looking into the raw data we can see that a good proportion of users have different passwords for different accounts and perhaps is a good explanation for the number of leaked passwords vs employees:

```
            (email : password)
              azim.door@3i.com : 540787life
              azim.door@3i.com : bzkat06
              azim.door@3i.com : beckham19
              azim.door@3i.com : Internet4
```

Using one password for everything is common practice for users with little security training but is a leading cause of data breaches. So is this a sign of good password hygiene for 3i? Perhaps. 3i rank below average at 25th on our FTSE100 list. I could only find one in-house cyber security engineer working at 3i on LinkedIn and I found the following statement from their latest financial report interesting: *"We continued to enhance our cyber security management and reporting and engaged an external firm to provide a dedicated Chief Information Security Officer service in the year. Due to the nature of our business,* ***cyber security is not considered a principal risk*** *but is included on our watch list and remains under regular review by the GRC and Audit and Compliance Committee."*

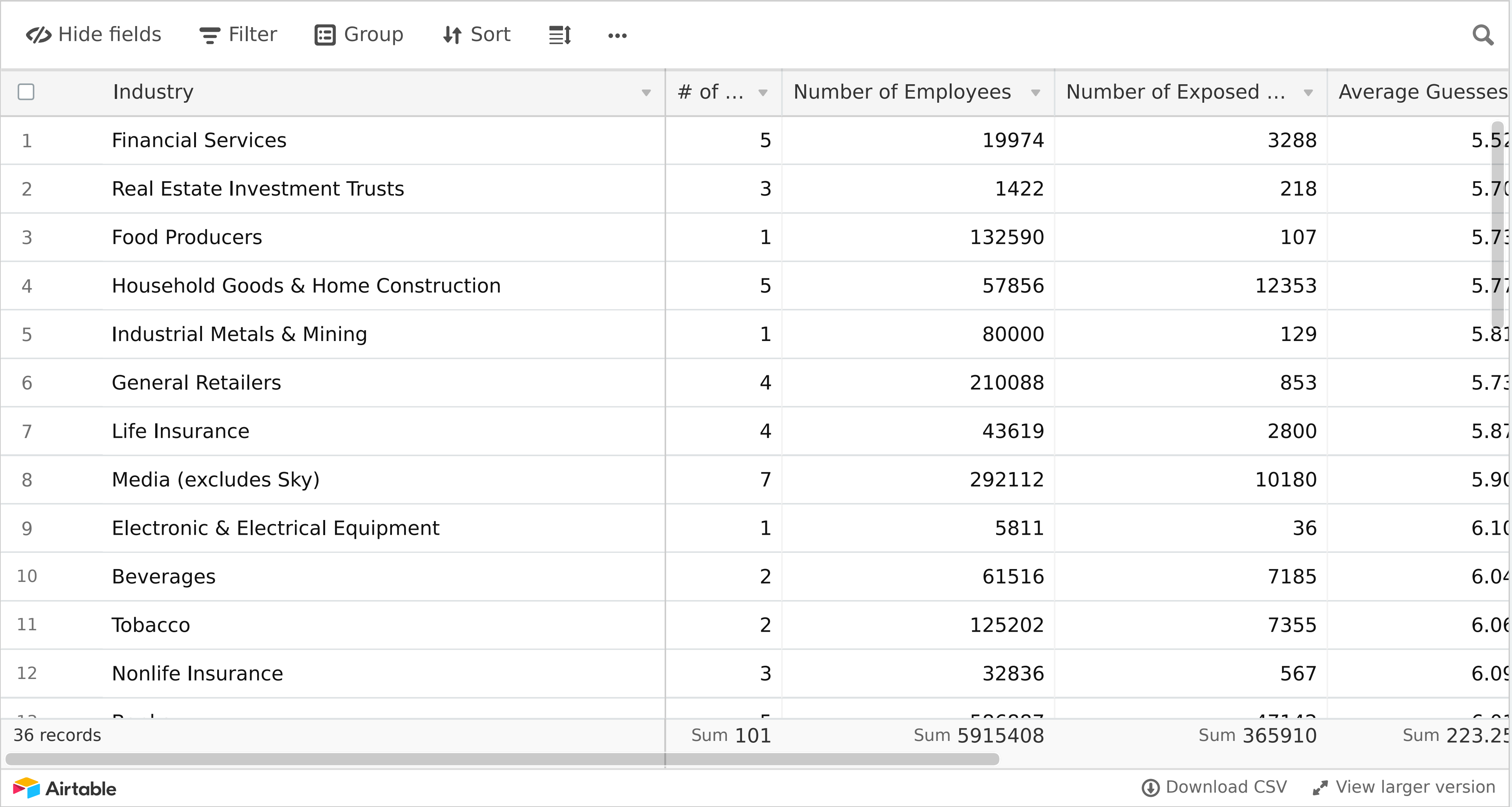
I would've thought that companies with less leaked credentials generally score higher but the data doesn't really show this. Bunzl and Barclays have only leaked 0.68% and 0.41% of their employees credentials but score 2nd and 3rd worst in password hygiene. Similarly, Shell rank fairly well at 86th best even though 1/4 of employees have leaked credentials (26.96%).

What about market cap? Does a company's higher market value (and by extension larger revenues) mean that they spend more on cyber security?



You can definitely see a slight upwards trend in higher password scores given a higher market cap.

Across the industries



	Industry	# of …	Number of Employees	Number of Exposed …	Average Guesses
1	Financial Services	5	19974	3288	5.52
2	Real Estate Investment Trusts	3	1422	218	5.70
3	Food Producers	1	132590	107	5.73
4	Household Goods & Home Construction	5	57856	12353	5.77
5	Industrial Metals & Mining	1	80000	129	5.81
6	General Retailers	4	210088	853	5.73
7	Life Insurance	4	43619	2800	5.87
8	Media (excludes Sky)	7	292112	10180	5.90
9	Electronic & Electrical Equipment	1	5811	36	6.10
10	Beverages	2	61516	7185	6.04
11	Tobacco	2	125202	7355	6.06
12	Nonlife Insurance	3	32836	567	6.09
36 records		Sum 101	Sum 5915408	Sum 365910	Sum 223.25

The Financial Services, Real Estate Investment Trusts, and Household Goods & Home Construction industries fair poorly in the bottom 4. Whilst the Pharmaceuticals & Biotechnology, Oil & Gas Producers, and Mining industries shine at the top. On the face of it, and without delving any deeper, it seems the companies in the bottom 20 percentile are less technology focused than the top 20 percentile - which makes sense.

But when you sort the data by the total number of leaked credentials per industry, Oil & Gas Producers and Pharmaceuticals & Biotechnology are in the top 3. Lots of leaked passwords, but relatively secure and good password hygiene.

For love and OSINT

Most people create passwords that are easy to remember which usually means it's based on something they love and value, e.g. their childs or dogs name followed by their age or year they were born. Or perhaps a special date or memorable place between two people. So I wonder if two people close to each other will share a password? We can cut and slice the data to remove the top 10,000 most common passwords, passwords with too much entropy (randomness), and passwords that either appear less than 3 times (too unique) or more than 10 times (not unique enough). This gives us some interesting insights.

Password `20limestreet` (which I'm assuming is an address) appears in our breach lists 6 times for 2 accounts: `virginia@branscomyellow.com` and `jane.brown@astrazeneca.com` . Using open source intelligence we can identify their LinkedIn profiles and they both appear to be from Boston, Massachusetts. By combing through their profile endorsements we can see that Virginia thinks highly of Jane. And this is the front of their house:

The password `HubbyWifey4ever!` appears 3 times in our breach lists and is linked to 2 accounts: an individual at Sage Group and another at Legal and General Group. Again, by using OSINT we can quickly link the two individuals on social media and confirm they are husband and wife.

Or perhaps we're trying to find out as much information as possible about the e-mail `rodrigo.digos2217@hotmail.com` and our usual OSINT avenues show up empty. Searching the breach lists returns just the 1 result

```
           (email : password)
rodrigo.digos2217@hotmail.com : $Rodrigozica0213
```

Pivoting on the relatively unique password returns two other accounts:

```
     (email : password)
   rodrigo.digos@sc.com : $Rodrigozica0213
rodrigo.digos@yahoo.com : $Rodrigozica0213
```

Now we know that Mr Digos works/worked at Standard Chartered and has a LinkedIn profile associated with his @yahoo.com e-mail address. Another example is the e-mail `kocak.sergi@gmail.com` and password `aitziber31bilbao` , which if we pivot on reveals the account `sergi.kocak@unilever.com` . And even within our FTSE100 data set there are many other examples, perfectly highlighting the problem of password reuse across personal and company accounts

In summary

You could spend a lot of time analysing the data and cutting and slicing it in different ways to extract intelligence. For example, it would be interesting to see if we could spot any trends depending if a company has in-house cyber capabilities and the size of their team. To summarise:

1. I was surprised to see the Financial Services sector come out the worst, especially given strict regulatory requirements and the large financial value of assets and portfolios managed.
2. From our external narrow view it looks like GVC Holdings and Ashtead Group are doing something right.
3. And we found that you can easily identify relationships between accounts and individuals based on passwords - our spam bot network or husband and wife for example. I wonder if you could extend this to identify corporate espionage, e.g. the same individual with two accounts using the same unique password both at Shell and BP?

Protecting your company

These breach lists are already out there and there will be plenty more to come. So what can you do? Specifically for passwords you should:

1. Teach your users what a good password looks like (hint: a long unique passphrase). Why is it important? Show examples of good and bad passwords. Make sure this advice is embedded within your induction programme for new joiners.
2. Audit passwords monthly to identify training needs for users who are still struggling to create strong passwords. Reward staff who are creating better passwords.

3. Stop forcing users to reset their password every X days. Yes, it reduces risk but at great cost. Research suggests this leads to users creating weaker passwords over time. Only force users to reset passwords if you believe they have been compromised.

And of course you should layer that with the usual additional security controls:

1. Ensure wherever a password is used externally, it has adequate security controls in place such as rate limiting and 2 Factor Authentication. Take into account other factors such as login time, geographical location, and IP address and deny login attempts if it falls outside of the user's usual pattern.
2. Gradually increase the minimum password length requirement to a minimum of 10, ideally 12, characters. Longer passwords increase entropy, which means they are (generally) more secure. Consider rolling out a password manager and adequate training to help with this.

Or give the Passlo platform a try with our 30-day free trial and we will take care of all the above.

***Please note**: All of this data is publicly accessible. I have changed certain characters where I have linked e-mails and passwords.*

← Back to the blog

Tweet Share

Enjoyed reading this article? Be the first to get the latest directly to your inbox.

Your e-mail address | Subscribe to newsletter

About 1 e-mail a week. Unsubscribe at any time.

About Passlo

Blog

Contact Us

Legal

Terms of Service

Privacy Policy

Get in touch

Passlo on LinkedIn

Passlo on Twitter

hello@passlo.com

+44 203 488 3744

Company number: 11323279. Registered office: 71-75 Shelton Street, London, United Kingdom, WC2H 9JQ

Passlo