vericlouds

More than 2,771,673 online account credentials linked to employees of Fortune 500 companies have been leaked.

VeriClouds Team
1/30/2018

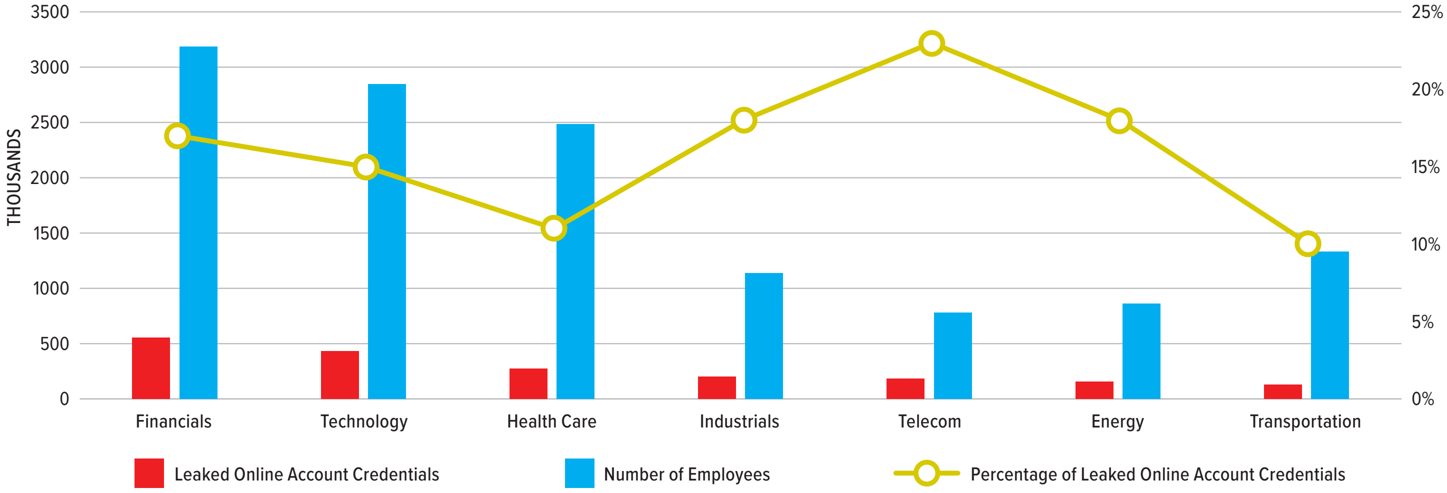
A backbone of our economy, Fortune 500 companies employ more than 27 million people. The online account credentials of **1 out of 10 employees of Fortune 500 companies have been leaked** to the dark web, resulting in the potential compromise of more than 2.7 million credentials, according to data analyzed by the VeriClouds research team.

This data was accumulated over **the past 3 years** and represents the largest available data repository of over **8 billion stolen credentials**. The VeriClouds team also analyzed the research by sector and industry, with some of the largest numbers coming from areas where leaked data can seriously impact customers, such as the Financials sector, and critical infrastructure, such as Energy.

Some industry sectors such as Telecommunications, Energy, and Financials have the largest percentage of leaked credentials compared to the number of their employees – 23%, 18%, and 17% respectively. The highest total number of leaked credentials are among the Fortune 500 companies operating in the Financial sector – over 555 thousand credentials or **20% of all leaked**.

Those numbers are disconcerting, since **the higher the number of leaked credentials at a company, the higher the risk of data breach**.

Fortune 500 Leaked Online Account Credentials



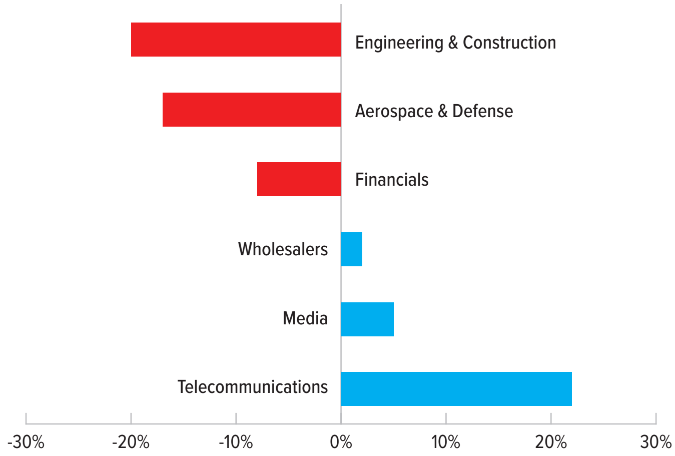
We see that on average each leaked Fortune 500 email address, associated with an online account, is found at 2.3 leaked data sources. This fact contributes to increased credential availability and makes it a preferred method for bad actors to breach organizations using credential stuffing or account takeover attacks. Furthermore, the availability of credentials data increases when many bad actors repackage or combine older breach data and resell it.

Personal online account credentials could be used in 'spear phishing' attacks against a device that is used for both work and personal use. If employees are allowed to use personal devices to access work resources, additional risk is posed to companies. The extend of such risk is unknown at this time and could be identified as part of another research.

In some cases, the Fortune 500 companies do not have control over the credential leaks. This is especially true if a Fortune 500 employee creates an account using the company's email address at a third-party online service. If the third-party service suffers a direct breach and its customer passwords are leaked, then we can assume that some of the same leaked passwords are used by employees at their Fortune 500 companies.

Our own customer research at a major airline company, done in second half of 2017, showed that approximately **13.1% of the leaked customer passwords found on the dark web matched the current passwords** of the airline's **customers**.

Growth leaked account credentials 2016 to 2017



> 13.1% of the leaked customer passwords found on the dark web matched the current passwords of a major airline's customers.
>
> — VERICLOUDS RESEARCH, 2018

Password strength influences the speed at which leaked passwords can be decrypted by bad actors. Our research shows that **some industries have a large percentage of weak**[1], **compromised passwords** – Computers, Office Equipment industry has **the largest percentage of weak, compromised passwords** with 25%, followed by Transportation Equipment and Telecommunications industries with 17.6% and 12.9% respectively. The Commercial Banks industry has **the highest total number of weak, compromised account passwords** with 109 thousand, followed by the Telecommunications industry with more than 100 thousand and Computer, Office Equipment industry with 73 thousand weak, compromised passwords.

The silver lining is that compared to 2016, **the number of online account credentials leaked on the dark web in 2017 across the Fortune 500 companies decreased by 7.5%**. Engineering and Construction, Aerospace and Defense, and Financials saw 19.5%, 17.2% and 7.7% decreases respectively. We don't know the specific reason for the overall decrease. One possible reason could be that some companies have applied more strict security policies to discourage employees using corporate email addresses to register accounts on 3rd party websites. We also noticed in 2017 some well-known dark web credential sellers disappeared from the market place. On the other hand, there were sectors, such as Telecommunications, Media and Wholesalers sectors, that **experienced increases in the number of leaked account credentials** in 2017, with 22.4%, 5.0% and 2.3% respectively.

The availability of over 2.7 million leaked online credentials of Fortune 500 employees increases their exposure to cybersecurity risk. The adequate measurement of this risk requires visibility over the extent of leaked online credentials as a result of third-party breaches, phishing, and malware. To address this risk, cybersecurity companies focus on credentials monitoring and verification, which takes the guesswork out of detecting compromised credentials and helps effectively automate the remediation.

[1] Part of the most common 100 thousand passwords from a database of more than 8 billion credentials.