TERBIUM LABS
Dark Web Data Intelligence

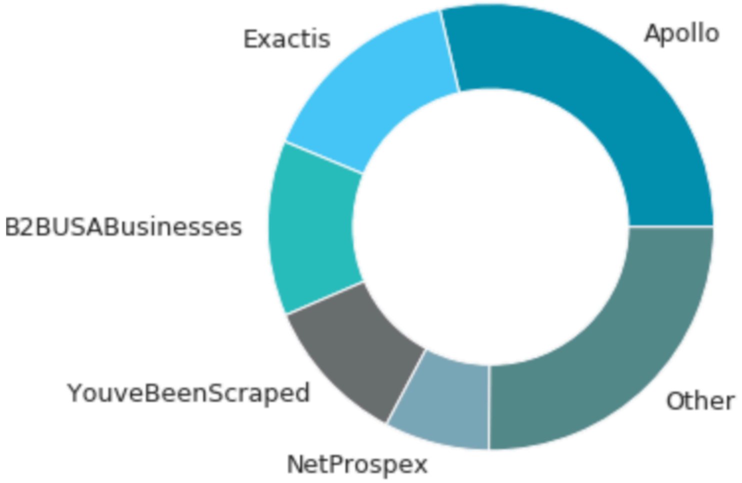
YouveBeenScraped Third Party Data Breach Analysis

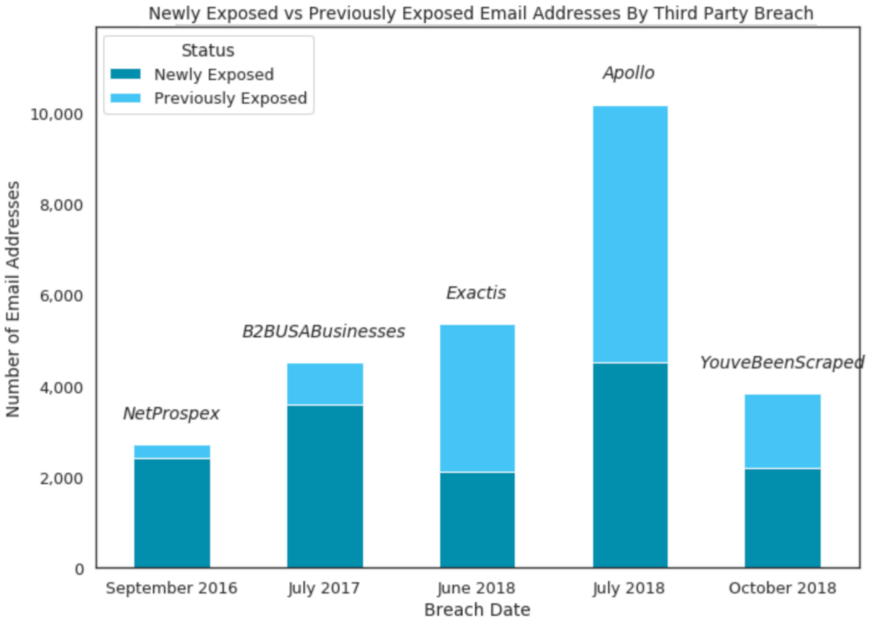
FINDING

According to Matchlight's index of third party breaches, the YouveBeenScraped data breach is the most recent third party breach affecting [CUSTOMER] domains — and the fourth largest to date.

ASSESSMENT

In November 2018, security researchers discovered an unsecured MongoDB database containing 66 million records, including work and personal email addresses, names, employers, physical addresses, job titles, and social media profiles.[1] Researchers have not identified the creator of the database, although the records within appear to be scraped from LinkedIn profiles. Within [CUSTOMER] domains, **3,825 unique email addresses** appeared in the YouveBeenScraped breach, making it the most recent and one of the top five biggest third party breaches affecting the company. For a complete list of exposed email addresses, see the csv "[CUSTOMER] YouveBeenScraped Email Addresses" uploaded to Matchlight on December 7th, 2018.





YouveBeenScraped **exposed [CUSTOMER] 2,169 email addresses** not seen in any previous third party breaches. [CUSTOMER] should monitor the email addresses included on this list for increased instances of spam and phishing attempts. This third party breach increases the total volume of data exposed but does not change [CUSTOMER]'s overall pattern of exposure in data types or distribution of email exposure.

Terbium Labs will continue to track the fallout from this third party data breach and update [CUSTOMER] with any modified or new findings accordingly.

[1] New Report: Unknown Data Scraper Breach, HackenProof, (December 2018) https://blog.hackenproof.com/industry-news/new-report-unknown-data-scraper-breach/