[CUSTOMER]

January 2019

MONTHLY REPORT

12-08-2018 TO 01-08-2019

TERBIUM LABS

Dark Web Data Intelligence

Executive Summary

This report evaluates [CUSTOMER]'s exposure based on **46** Fingerprinted records in **one** group, **four** data feeds, and **12** monitored email domains.

During this reporting period, analysts reviewed **608** matches on [CUSTOMER] terms, and found **14** mentions tied to [CUSTOMER].

MATCHLIGHT RESULTS OVERVIEW

Matchlight discovered two phishing email lists on Pastebin containing six [CUSTOMER DOMAIN] email addresses.

- Email address lists could be used to potentially phish [CUSTOMER]'s employees.

Matchlight also discovered mentions of [CUSTOMER] and [SUBSIDIARY] on eight doxing posts.

- This series of posts call for a citizen's arrest of individuals and organizations associated with an obscene website and does not focus on [CUSTOMER] as an organization.

THIRD-PARTY BREACH EXPOSURE OVERVIEW

- **64.94%** of [CUSTOMER]'s exposed email addresses appeared in 2018. This exposure was primarily caused by the *Exactis*, *Apollo*, and *YouveBeenScraped* third party breaches.
- While [CUSTOMER] email addresses did not appear in any third party breaches over this reporting period (12-08-2018 to 01-08-2019), over the last three months [CUSTOMER] domains appeared in three third party breaches.
- **83.5%** of the email addresses exposed in this three month period were exposed alongside data types that would enhance phishing attempts. No passwords, either hashed or plaintext, were exposed during this three month period.

RECOMMENDATIONS

The CSV uploaded to the Matchlight dashboard includes relevant metadata associated with third party breaches affecting your organization's email domains in the last three months. For each unique email address affected by a breach in this time period, the document lists the following:

- most recent breach name and date (Column G & J)
- exposed data types for this time period (as well as all time) (Column I & M)
- whether hashed or plaintext passwords were released (Column C & D)
- if email and job title were exposed during this time period, we mark this email as at risk for phishing (Column E)

Terbium Labs recommends **resetting passwords for accounts that have had hashed or plaintext passwords exposed during this time period,** as well as for any accounts exposed for the first time. Additionally, we recommend **phishing monitoring for email addresses exposed with data types such as occupation or job title,** as well as providing updated or additional anti-phishing training to targeted employees.

Matchlight Findings

FINDING

Matchlight detected the email address [NAME@DOMAIN.COM] on a post on Pastebin that was immediately removed with no cached copy available for analysis. Matchlight also detected [NAME1@DOMAIN.COM], [NAME2@DOMAIN.COM], [NAME3@DOMAIN.COM], [NAME4@DOMAIN.COM], and [NAME5@DOMAIN.COM] on an email list consisting of 5,656 email addresses. The majority of the email addresses in this list are personal, e.g. Hotmail, Yahoo, AOL, but the post also includes education, military, government, international, and corporate domains. This list has also been removed.

ASSESSMENT

Neither of these lists focus on [CUSTOMER]. The leaks that occurred during this period are of a frequency and in a format that Terbium Labs would expect for for an institution of [CUSTOMER]'s size, but [CUSTOMER] should assess these email addresses to determine if these accounts have privileged access to company data, notify employees of possible phishing attempts, and issue password resets for these accounts if necessary.

SOURCE

See Appendix, Section 1

FINDING

A series of doxing posts calling for a citizen's arrest of individuals and organizations associated with specific prostitution websites includes a retired [CUSTOMER] Vice President, but does not include any other personal information or other references to [CUSTOMER].

ASSESSMENT

These posts, titled "Citizens arrest of myredbook.com", lists Fordham University's Board Members, including "[EXECUTIVE'S NAME], [SUBSIDIARY], A [CUSTOMER] Company". The unidentified poster calls for a citizen's arrest for a broad range of people associated with Fordham University as well as the Los Gatos police department and alleges their connection to the former myredbook.com, now providingsupport.com, a prostitution website.

These posts are slightly different than posts discussed in [CUSTOMER]'s October 2018 report, and do not include any other personal information associated with [EXECUTIVE'S NAME] or any other references to [CUSTOMER]. It is unlikely that this post constitutes a credible threat to any individuals' personal safety.

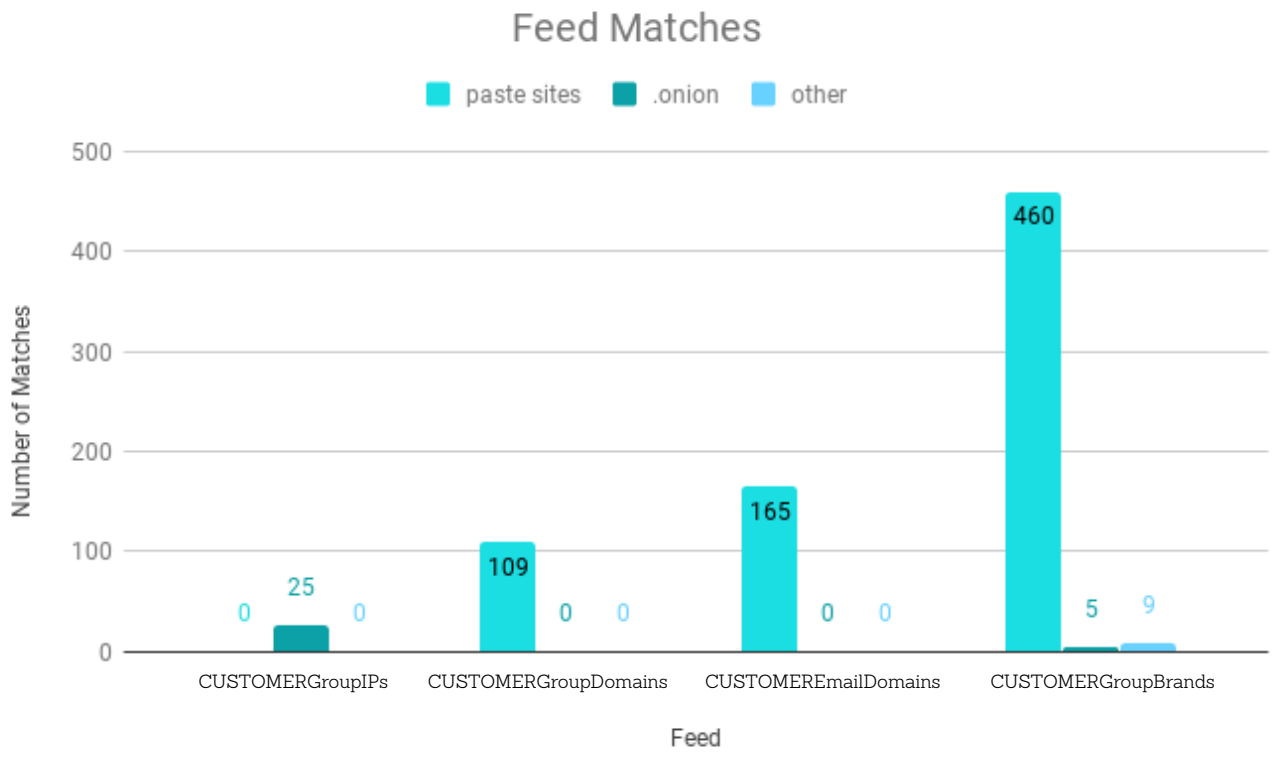
SOURCE

See Appendix, Section 2

FEED MATCHES

[CUSTOMER]'s domain, brand, and IP feed matches are shown in the graph below, along with where on the dark web they were discovered. [CUSTOMER]'s brand feed, on the far right, produced a large number of matches due to "[CUSTOMER]" appearing in multiple company names, e.g. Encore [CUSTOMER], DC [CUSTOMER], etc. 97% of these matches appeared on Paste sites like Pastebin. [CUSTOMER]'s IP address feed on the far left, produced the largest number of matches on onion sites due to public IP address lists on the Tor Project's git repository. The IP address XXXX:XX:XXXX:ffff:ffff:ffff:ffff:ffff appears on multiple lists of public IPv6 blocks with associated geolocations. These lists are not malicious and do not mention [CUSTOMER].

Terbium Labs constantly assesses feed results and works to refine feeds to eliminate noise. Please review your feed terms under monitoring listed in the Appendix to ensure terms are up to date and accurate.

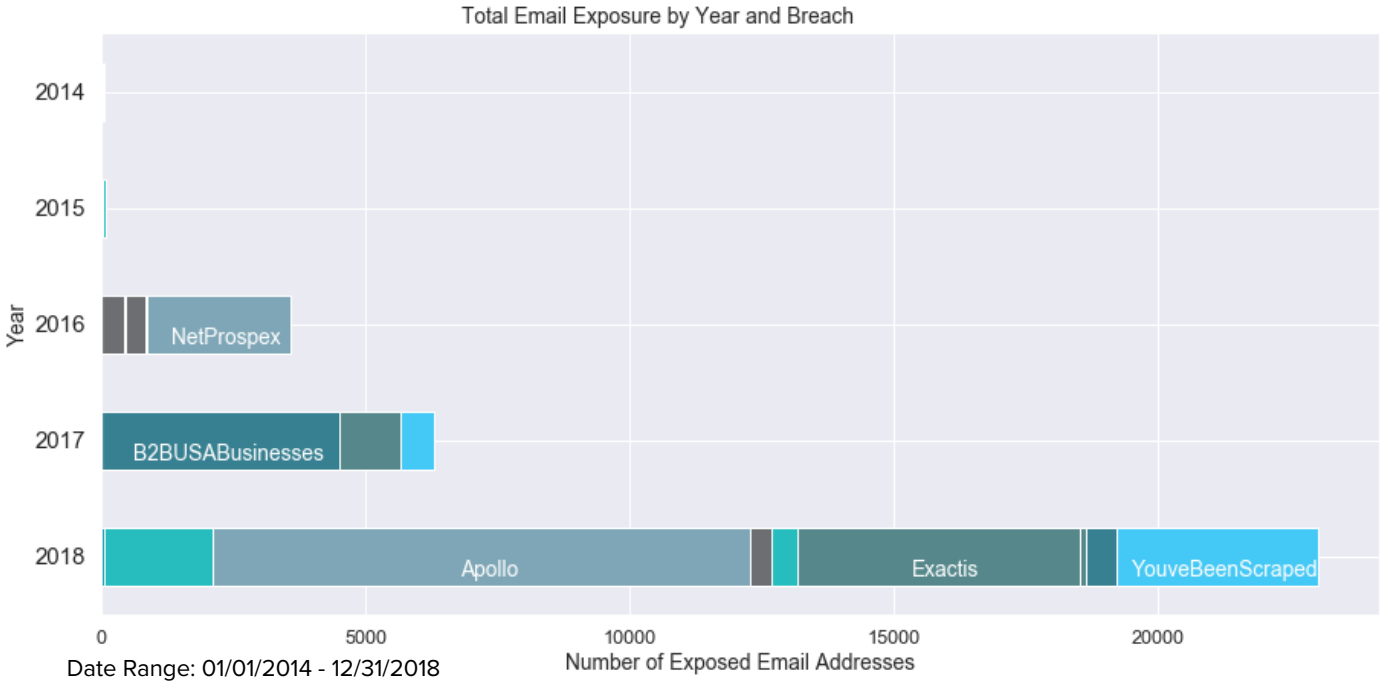


Your organization has uploaded very few Fingerprinted PII records to Matchlight. For additional PII monitoring, consider uploading records for privileged access employees, such as IT or Finance individuals. Please see "Records Monitored" in the Appendix for PII monitoring suggestions. Terbium Labs can also work with you to define other persons of interest and provide guidance on the most effective categories and uploading strategies upon request.

Third Party Breach Exposure

THIRD PARTY BREACH EXPOSURE BY YEAR

[CUSTOMER]'s overall third party exposure has increased over the past five years: **64.94%** of [CUSTOMER]'s exposed email addresses appeared in 2018, with three of [CUSTOMER]'s top five breaches by volume — *Apollo*, *Exactis*, and *YouveBeenScraped* — appearing that year. Terbium Labs has observed a similar trend for other organizations. The graph below shows [CUSTOMER]'s email address exposure from 2014 to 2018, with the top five breaches labeled. Note that this graph shows total exposures of email addresses, not unique exposures.



Date Range: 01/01/2014 - 12/31/2018

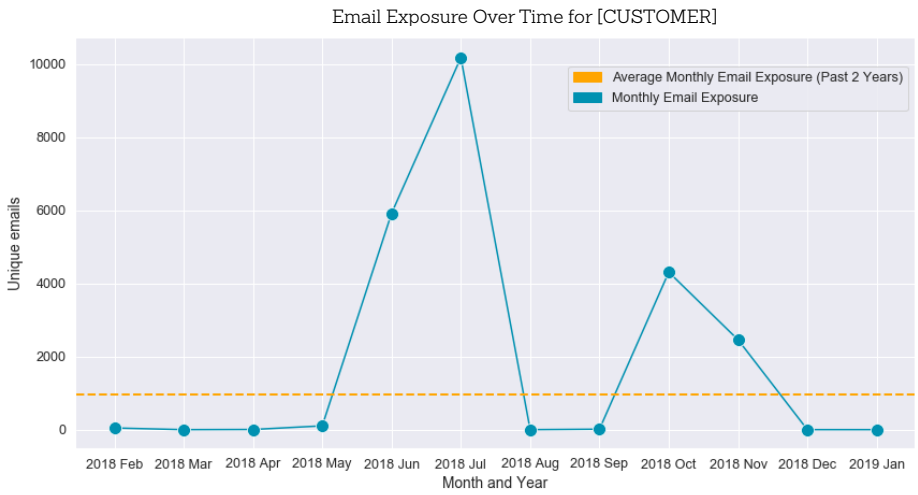
One of the biggest breaches of 2018, *Exactis*, occurred in June, exposing more than 340 million records. This third party breach exposed a wide range of data types, including but not limited to **credit status information, dates of birth, education levels, email addresses, ethnicities, family structure, financial investments, genders, home ownership statuses, income levels, IP addresses, marital statuses, names, net worths, occupations, personal interests, phone numbers, physical addresses, religions, and spoken languages**.

In July 2018, the sales engagement startup *Apollo* publicly exposed a database containing billions of datapoints attached to 126 million email addresses. This third party breach exposed information from *Apollo*'s prospect database: **names, email addresses, employers, employee roles, and physical work addresses**. In a statement, *Apollo* clarified that the data did not include information such as account credentials, Social Security numbers, or financial data.

The *YouveBeenScraped* breach was identified 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**. Researchers have not identified the creator of the database, although the records within appear to be scraped from LinkedIn profiles.

THIRD PARTY BREACH EXPOSURE OVER THE LAST 12 MONTHS

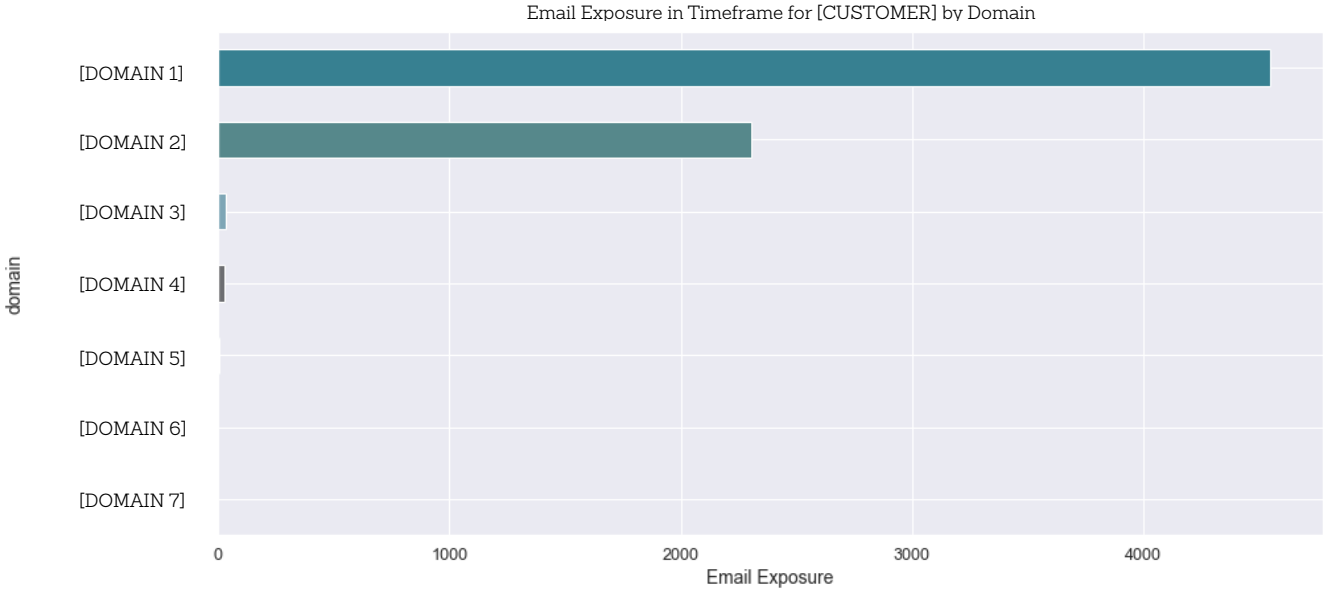
As the graph to the right shows, the bulk of [CUSTOMER]'s exposure over the last 12 months occurred with the *Exactis* breach in June 2018, the *Apollo* breach in July 2018, the *YouveBeenScraped* breach in October 2018, and the *Adapt* breach in November 2018.



In almost all other months, the number of exposed [CUSTOMER] email addresses was zero or near zero. This pattern shows that [CUSTOMER] is not affected by constant low or medium level third party breaches, but rather is exposed in larger events only a few times a year.

THIRD PARTY BREACH EXPOSURE BY DOMAIN IMPACTED

Over this 12 month period, the majority (**65.69%**) of the [CUSTOMER] email addresses exposed had the domain [DOMAIN 1], followed by [DOMAIN 2] (**33.28%**), [DOMAIN 3] (**0.49%**), [DOMAIN 4] (**0.39%**), [DOMAIN 5] (**0.08%**), and [DOMAIN 6] and [DOMAIN 7] (**0.03%** each). Your organization should verify that this distribution matches the distribution of email addresses issued. If one domain is overexposed, that merits further investigation.

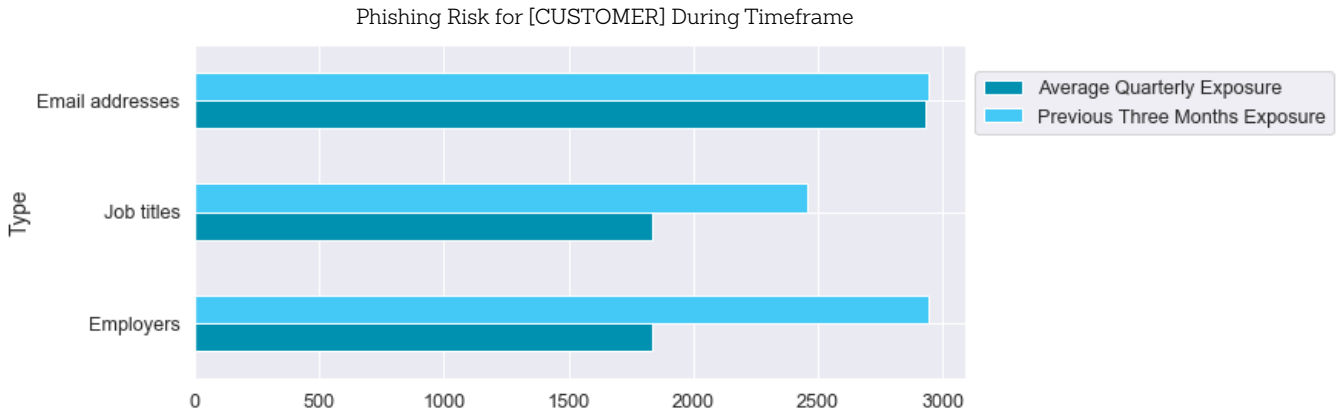


Date range: 10/08/2018 - 01/08/2018

THIRD PARTY BREACH EXPOSURE BY TYPE OF DATA

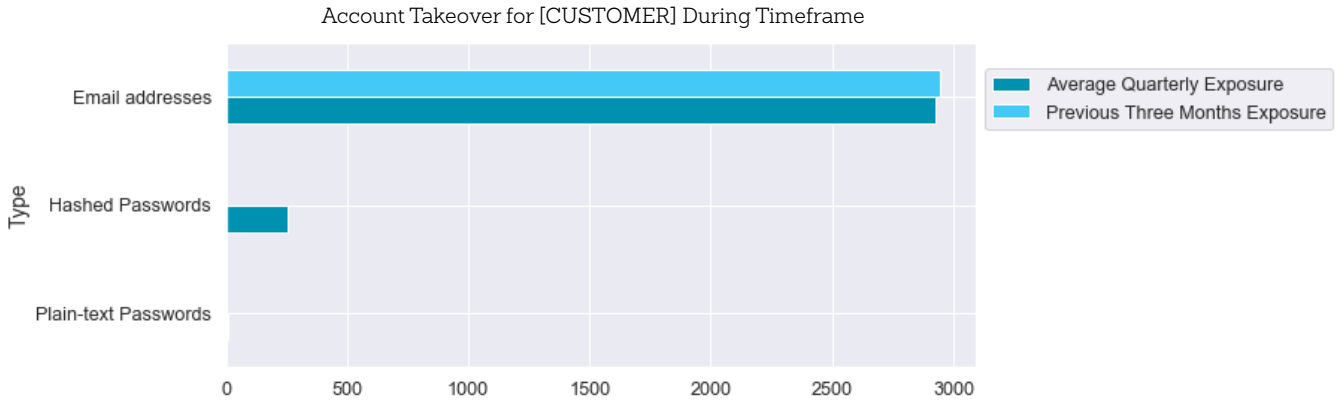
Phishing Risk

While phishing attacks can exploit email addresses that were exposed without other data types, fraudsters can enhance their phishing emails by using other information about their targets like job title or employer name. **83.5% of your exposed emails were exposed with data types that put them at risk for potential phishing attacks.** [CUSTOMER] can find these at risk individuals using Column E of the CSV uploaded to Matchlight.



Account Takeover Risk

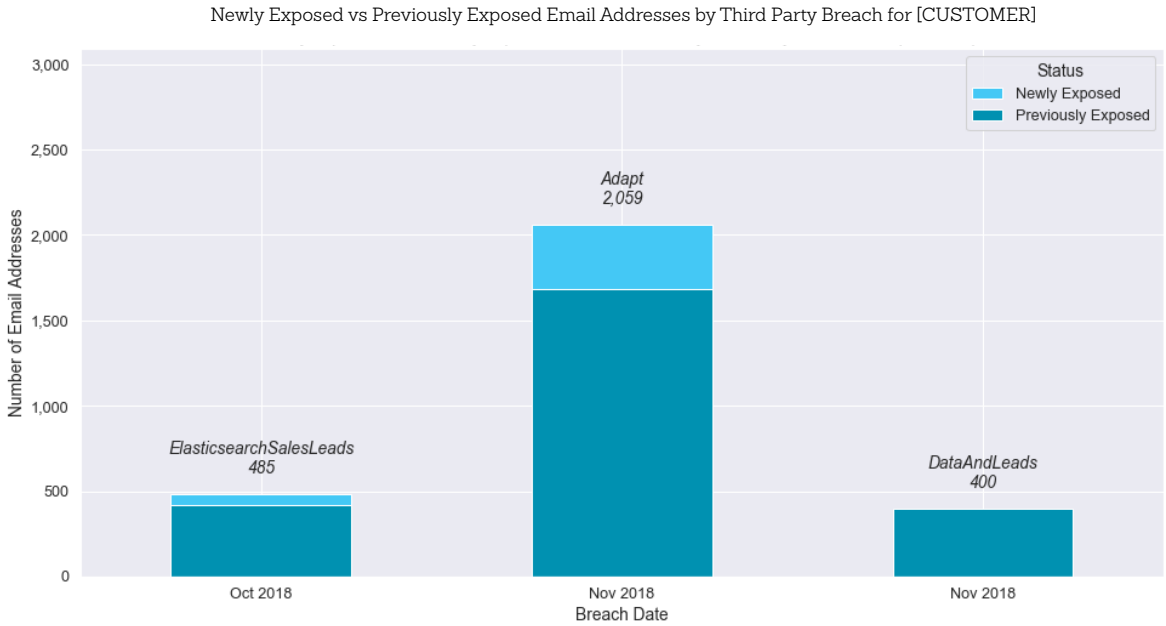
Criminals can decipher some hashed passwords using databases of previous hacks. Internal policies, like initiating password resets after emails are discovered in third party breaches, can reduce the risk that one of these credential sets will allow a criminal to access sensitive accounts. **0% of your email addresses exposed over the last three months were exposed with hashed or plaintext passwords.**



Date range: 09/01/2018 - 01/08/2018

HIGH EXPOSURE THIS QUARTER COMPARED TO QUARTERLY AVERAGE

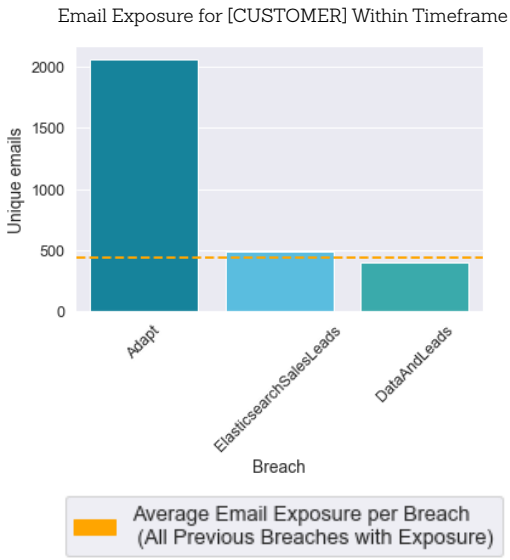
As the graphs on the previous page show, over the past three months, [CUSTOMER] email addresses **had a higher than average exposure** in third party data breaches. However, none of these breaches occurred during this reporting period (12-08-2018 to 01-08-2018).



This graph shows the distribution of newly and previously exposed email addresses in the past three months.

As the graph below shows, the average third party breach affecting [CUSTOMER] exposes **439** individual email addresses. *Adapt* exposed more email addresses than the average third party breach. The three third party breaches affecting your organization's email addresses in the past three months included mostly email addresses that had been exposed in previous third party breaches.

Two of the three third party breaches affecting [CUSTOMER] in the last three months (*ElasticSearchSalesLeads*, and *DataAndLeads*) contained more than 50 million records. *Adapt* contained more than nine million records. While third party breaches of this size do not target your organization specifically, the size and frequency of these third party breaches can still put your organization at risk of phishing and spam attacks.



Date range: 10/08/2018 - 01/08/2018

COMPARATIVE ANALYSIS OF EXPOSURE

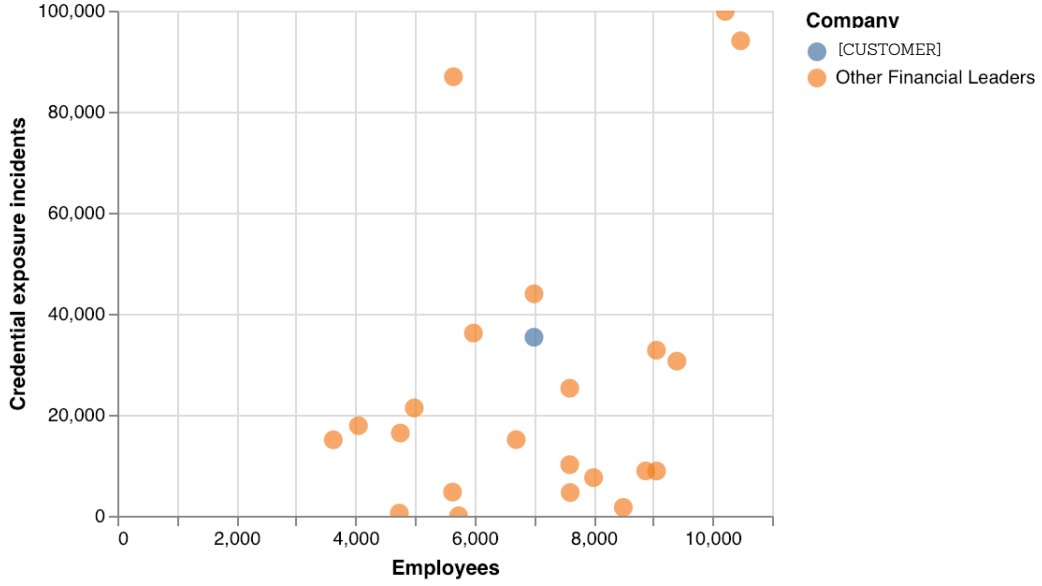
Establishing a baseline level of exposure is a crucial part of evaluating an organization's risk profile. While every organization is unique, comparing to competitors or industry leaders provides valuable insight into an organization's relative exposure.

Terbium Labs analyzed [CUSTOMER]'s email domain exposure in third party breaches against 22 industry competitors. **Based on 12 email domains** (see Appendix), **[CUSTOMER] has more exposed emails per employee than 77.27% of the leaders of comparable size in your industry.** This is a high level of exposure relative to other financial leaders of similar size. Please contact Terbium Labs if your total number of employees or individuals with a [CUSTOMER] email domain is incorrect so we can provide the most accurate analysis.

The chart below shows [CUSTOMER] (in blue) plotted against other financial companies (in orange). The horizontal axis shows each organization's total number of employees, while the vertical axis shows the number of exposed email addresses. Note that this is not the number of unique emails that have been exposed — due to credential reuse across sites and the repackaging and releasing of old credentials as part of new breaches, a single set of credentials can be exposed through multiple third party breaches.

The more frequently that an organization's email addresses appear in third party data breaches, the more likely that a cybercriminal will discover them. A higher exposed email address to employee ratio means that a large portion of your organization has been exposed through third party breaches. After the initial breach or exposure, cybercriminals resell and re-share compromised data many times across the dark web and in criminal communities, leading to increased phishing, spam, and malware attacks over time.

Exposure Incidents to Number of Employees for Financial Industry Leaders of Comparable Size (22 Competitors)



Date range: 01/01/2014 - 01/08/2018

Appendix

MATCHLIGHT FINDINGS:

Section 1:

hxxp://pastebin.com/path1

hxxp://pastebin.com/path2

Section 2:

hxxp://pastebin.com/path3

hxxp://pastebin.com/path4

hxxp://pastebin.com/path5

hxxp://pastebin.com/path6

hxxp://pastebin.com/path7

hxxp://pastebin.com/path8

hxxp://pastebin.com/path9

hxxp://pastebin.com/path10

RECORDS MONITORED:

Number of customers: 0
Number of employees: 0
Number of executives/VIPs/high value individuals: 46
Number of privileged access IT employees: 0
Number of privileged access Finance employees: 0