Pulse Report:
Spike In Credential Leaks for the Pharmaceutical and Biotech Industry

Recorded Future noted a spike in the relative number of credential leaks from the pharmaceutical & biotechnology sector compared to all credential leaks between November of 2019 and March of 2020. The number of credentials that are leaked vary greatly from month to month, a large credential dump can cause numbers for a given month to increase dramatically, and many of those credentials may be repackaged from previous leaks. That is why this report looks at the percentage of leaks tied to the pharmaceutical and biotech industry, rather than the absolute numbers, as it provides a more accurate picture of the situation.

Figure 1 shows the leaked credentials from the pharmaceutical & biotechnology industry tracked by Recorded Future between April 1, 2019 and April 30, 2020.

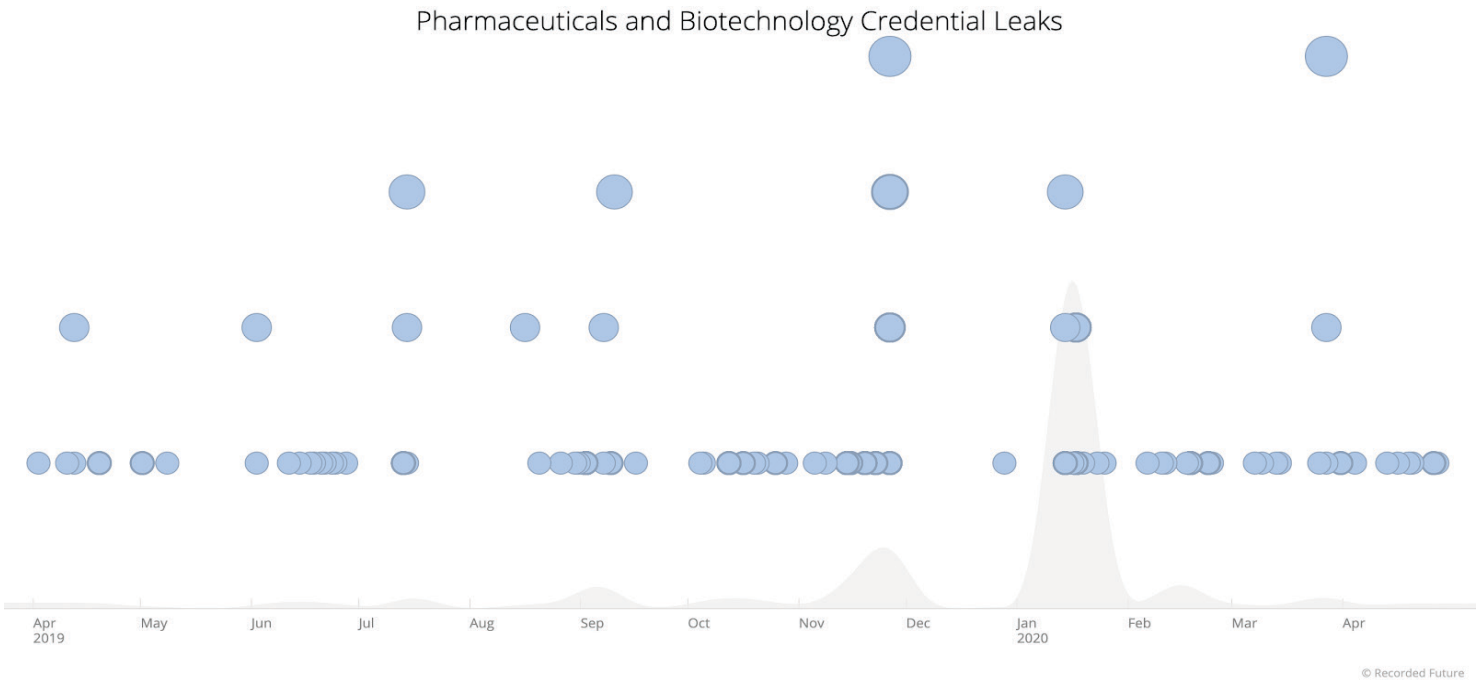

Figure 1: Leaked Credentials From the Pharmaceutical & Biotechnology Industry
https://app.recordedfuture.com/live/sc/3LfNLklXSh4L

Overall, the pharmaceutical and biotechnology industry accounted for .07% of leaked credentials during this period. However, there was a noticeable jump starting in November of 2019 and ending in February, which significantly skewed the average — the median percentage during this time is .03%.

Figure 2 shows the percentages of leaked credentials belonging to accounts tied to the pharmaceutical and biotechnology industry. November of 2019 saw the percentage jump to .24%, then the percentage reverted to the median of .03% in December, and it then jumped to .07% in January, .11% in February, and .06% in March. These are statistically significant increases. So, while the percentages of leaked credentials belonging to accounts associated with the pharmaceutical and biotechnology industry is small overall, there was definitely a significant increase.

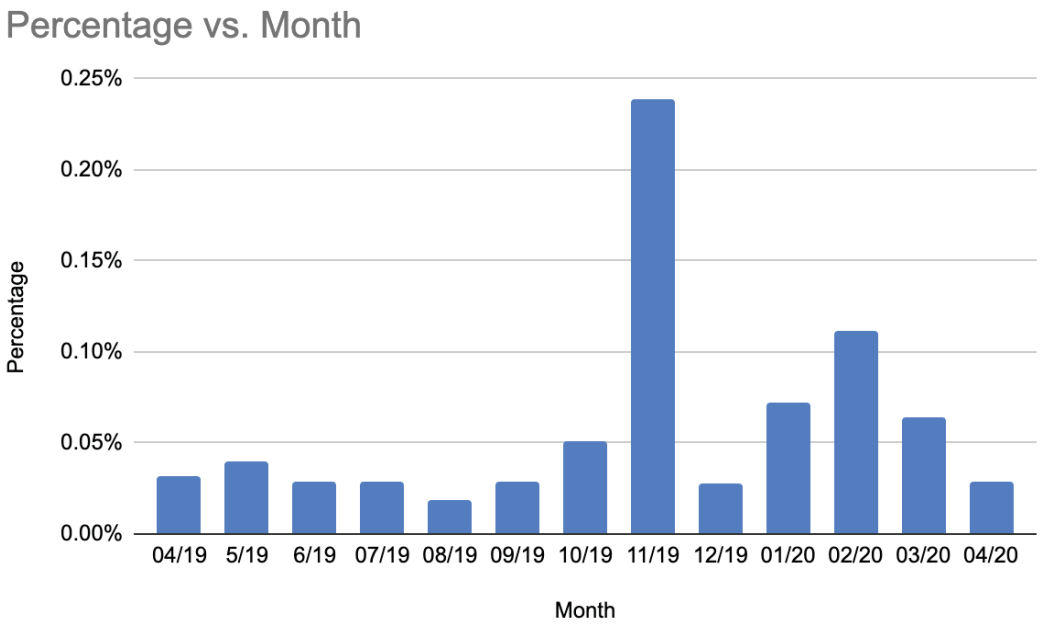

Figure 2: Percentage of Credential Leaks Belonging to the Pharmaceutical and Biotechnology Industry

In reviewing reports of large credential dumps, there do not seem to be any that were specific to the pharmaceutical and biotechnology industry during that period. An industry-specific credential dump would normally account for a spike in percentage. At this point, there is not a definitive answer as to why the spike occurred during this period, and any explanation based on available data would be pure speculation. That being said, given the statistical significance of the spike, it is unlikely that the increase was random chance.