



Finding the needle in the cyber haystack

# CRITICAL MANUFACTURING SECTOR DIGITAL EXPOSURE SUMMARY

Dexpose.io  
info@dexpose.io

Release Date  
2022-10-22

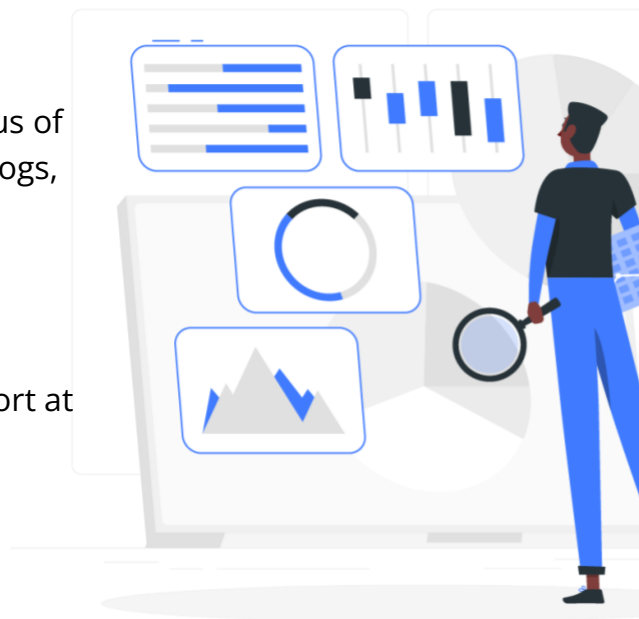
Classification  
Public report

# Executive Summary

The following report summarize the exposure status of the mentioned sector over the darkweb, malware logs, and publicly breached databases.

This report is part of DeXpose team research to enhance the Egyptian startup security status.

For more details we advise you to read the full report at [blog.dexpose.io](https://blog.dexpose.io)



## Key Findings

### Overall Severity

# Critical



**Sector:** Critical manufacturing sector



**Startups count:** 224



**Last Alert:** 2 days ago.



## 164

Startup mentioned in  
breached database

37 unique sources



## 115

Mentions in malware logs

N/A unique assets

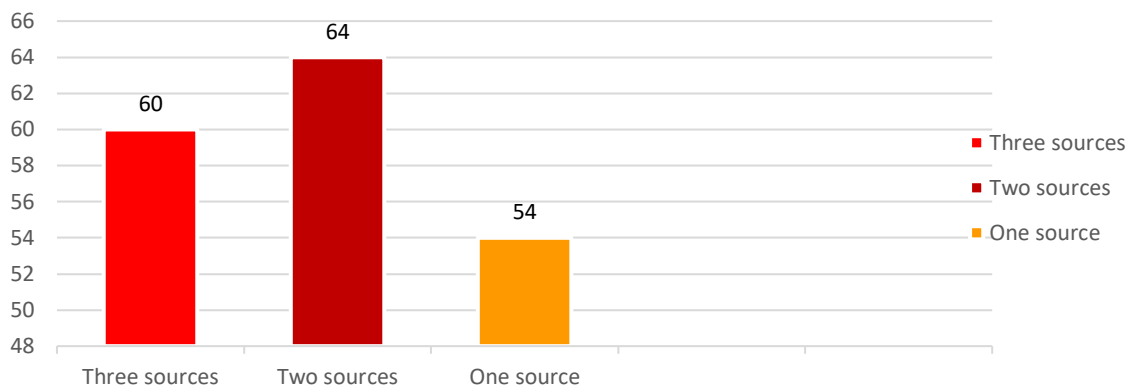


## 83

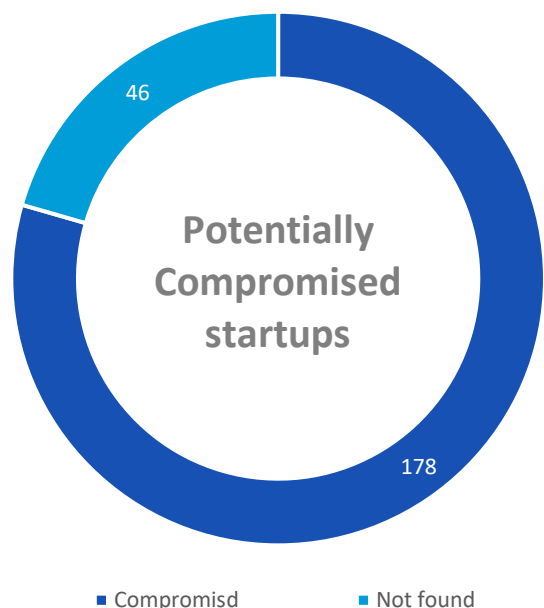
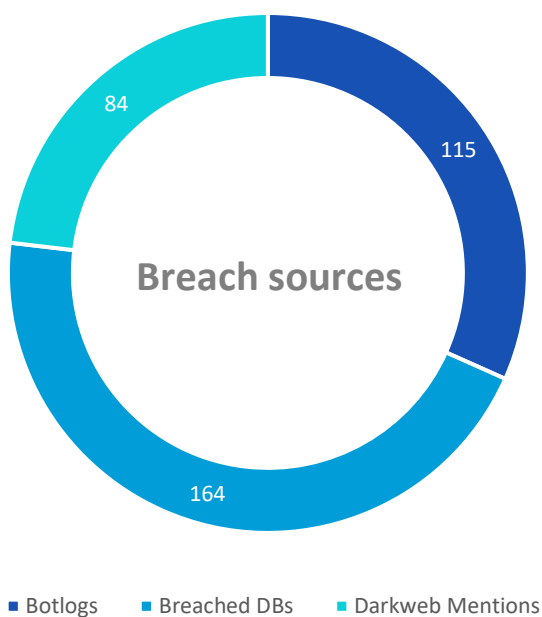
Dark/deep web marketplaces  
Mentions

3 unique sources

## Statistics



Distribution of startup breaches according to number of sources



- 60 startups were mentioned in three sources, which show high probability of compromise.

178 startups have at least one username or web service mentioned in the breach sources.



Your comprehensive digital risk monitoring partner that helps you identify multi-vector cyber threats and generate actionable insights to help you gain advantage over adversaries and proactively mitigate the risks.

## Why DeXpose?



### **Beyond Automation**

Hybrid approach of automation and human intelligence delivering the best coverage with sharp precision.



### **Deep investigation**

Investigating and reaching out potential threat actors possessing possible records related to your organization



### **Complete digital footprint**

Multiple modules covering your human and digital assets exposure over the internet



### **Continuous innovation**

Innovative technologies and services with continuous improvement to help enhance your proactive fighting against threat

[GET A SAMPLE REPORT TODAY](#)

