Scoring Compromised Credentials Risk

Score compromised credentials risk using three simple indicators

1. Percentage of Compromised Credentials

Calculated by matches an organization has divided by the organization's total pool of credentials with each credential weighted by category. Recommended is a weight of ten (10) for privileged credentials, five (5) for non-user ID and power user credentials, and one (1) for non-privileged credentials:

$$\frac{(1N+5N+10N)}{T} = \text{Aggregate } \%$$

Percentage of Compromised Credentials	Risk
> 70%	Maximum
51% - 70%	Very High
31% - 50%	High
11% - 30%	Medium
< 11%	Low

2. Availability of Compromised Credentials

Availability is linearly determined and calculated to an aggregate percentage across all credentials:

Available Now?	Has Been Available	Risk
Yes	3 months or longer	100%
Yes	More than 2 weeks but less than 3 months	80%
Yes	Available for the last 2 weeks	60%
No	3 months or longer	50%
No	More than 2 weeks but less than 3 months	30%
No	Available for the last 2 weeks	10%

3. Percentage Convertible Into Plain Text

Percentage of all passwords convertible to plain text as a linear aggregate percentage:

Percentage of All Credentials Convertible	Risk
>= 85%	Maximum
51% - 84%	Very High
21% - 50%	High
1% - 20%	Medium
0%	Low

Risk Surface

Once all risk scoring for compromised percentage, availability and plaintext percentage is known, then the scores can be triangulated according to the three points in a spider chart to visualize the total risk surface.

A sample is provided here for visualization.

Risk of Leaked Credentials

Percentage leaked credentials

100%
80%
60%
40%
20%
0%

Percentage plain text   Availablity