Mandiant

SUSPECTED ATTRIBUTION

Threat activity that Mandiant Threat Intelligence assesses with full confidence to be attributed to a named APT (state sponsored), FIN (financially motivated), TEMP, or UNC group will be marked **Mandiant Confirmed**. In some cases, we have evidence that activity sets may be related to existing groups, but not enough information to attribute the activity to the original group with full confidence. These activity clusters will be marked as **Mandiant Suspected** or **Possible Association** to indicate how likely we believe the activity to be related to the named group. **Mandiant Suspected** indicates that we have high or moderate confidence of a link; **Possible Association** indicates a low confidence association.

Our **Mandiant Suspected** and **Possible Association** assessments are based on the quantity and strength of overlaps between a cluster of activity and a named group. For example, **Mandiant Suspected** tags may refer to overlaps based on high quality information with multiple overlapping data points whereas **Possible Association** can be reflective of assessments based on single overlaps, similarities in generic TTPs, or identified commonalities where we have limited visibility.

Mandiant Advantage users, based on their unique use cases, will be able to select whether they want to consider the narrowest and highest fidelity set of information related to an actor (for example, only **Mandiant Confirmed** activity, or activity attributed to APT41 with full confidence). Users may also choose to widen their view to include **Mandiant Suspected** or **Possible Association** data.

Suspected Attribution Terms	
Mandiant Confirmed	Full confidence attribution
Mandiant Suspected	Moderate or high confidence attribution
Possible Association	Low confidence attribution