Mandiant

HOW DOES MANDIANT TRACK THREAT ACTORS?

As we detect and uncover malicious activity, we group forensically related artifacts into "clusters." These clusters indicate actions, infrastructure, and malware that are all part of an intrusion, campaign, or series of activities which have direct links. These are what we call our "UNC" or "uncategorized" groups.

Over time, these clusters can grow, merge with or break off from other clusters, potentially combined under a TEMP name, and eventually graduate into fully defined and publicly announced named groups, such as APT41 or FIN11.

This graduation occurs only when we understand enough about their operations in each phase of the attack lifecycle and have associated the activity with a state-aligned program or criminal operation.

As a group becomes sufficiently mature, the actor will be assigned a formal APT or FIN number. APT (Advanced Persistent Threat) groups are nation-state actors generally focused on espionage activities. FIN groups are highly organized criminal groups that engage in high-level financial crime such as business email fraud and extortion activities such as ransomware. The methodology for naming an APT or FIN group is identical in nature. One example of maturity is that there is enough evidence to believe the cluster activity represents an actual group, with confidence that the activity is not part of an existing group.

The name of a group can signify the motivations of the group:

- **UNC** - "Uncategorized" activity cluster; a starting point for building future analysis
- **TEMP** - TEMP groups can be considered equivalent to a significant UNC group
- **APT** - Activity cluster believed to be state sponsored and primarily focused on espionage
- **FIN** - Activity cluster believed to be primarily focused on financial gain that is not state sponsored

To learn more:

https://www.mandiant.com/resources/how-mandiant-tracks-uncategorized-threat-actors