Webinar Summary: Uncovering ICS Threat Activity Groups

dragos.com/blog/industry-news/webinar-summary-uncovering-ics-threat-activity-groups/

January 30, 2019

Activity Group: *a set of intrusion events related with varying degrees of confidence by similarities in their features or processes used to answer analytic questions and develop broad mitigation strategies that achieve effects beyond the immediate threat.*

Information security is inundated with activity groups and their menagerie of names: OBSIDIAN, APT8F9, FUZZYSNUGGLYDUCK, and their ilk. Some denounce these names as nothing but marketing fluff, others as the bane of their existence. But they play a very important role misunderstood by many and misused by more. This is the story of activity groups: what they are, how they're made, and how they should be used.

Activity groups are not created by some evil marketing genius, but instead part of the natural analysis process using a trait in human cognition to group like-elements together allowing us to identify patterns, provide perspective, and make better decisions over many individual elements. Analysts across almost every field of study use this technique – that of grouping, classification, and correlation.

Intrusion analysts create ***activity groups***: separate-but-somehow-related elements of computer and network intrusions clustered together to solve some analytic problem. The concept is not novel but was first defined in the Diamond Model of Intrusion Analysis. Analysts give these groups labels for the purpose of easy communication.

Creating and Managing Activity Groups

Creating activity groups well is not easy. An activity group must be driven by an analytic problem and the necessary data and relations to address the problem. Just as any scientist must first generate hypotheses, experimental frameworks, and gathering the necessary data, the intrusion analyst must first ask "what am I trying to accomplish?"

From this problem analysts create a "grouping function" (usually this is done mentally) to identify the features to compare (such as same IP/Domain, same file hash) and the confidence necessary (e.g., are two IPs in the same class C subnet going to be related in the group?). The analyst then groups all of the related events and follows by finally asking the question and coming to a conclusion – or going back for more data.

Activity groups are not static! In fact, over time and as the number of elements grows, the confidence that the group still accurately addresses the question declines. So, activity groups should change over time – be redefined and "retired" when no longer needed, have ceased to deliver new data, or outlive their usefulness. Unfortunately, we see many groups live well beyond their time and scope harming our ability as a community to generate meaningful conclusions.

Using Activity Groups

Defenders should look to activity groups in order to help derive effective and efficient mitigation strategies. They should group threat behaviors to identify the fewest mitigation actions necessary to achieve protection against the largest number of groups (e.g., the top 10 security controls). Defenders should extract intelligence from activity groups to inform red-teams, blue-teams, and the purple-teams in-between.

One of the most commonly seen analytic problems to use activity groups publicly is to identify a set of infrastructure and capabilities most likely used by the same set of operators. This grouping then commonly extends into attribution – the "whodunit" of threat intelligence questions. But there are many questions addressed by activity groups, including:

- Attribution: which activity is caused by the same set of organizations or operators?
- Malware authorship: which malware could potentially be authored by the same developer?
- Trending: How have events changed over time?
- Cross-capability: Which disparate activities show usage of common capabilities?
- Center of gravity: Which processes are common across the largest set of activity groups?

Many people identify activity groups only with attribution thinking the name of a group is nothing by a synonym for the group, organization, or individuals behind the activity. This is a mistake. There is no one way to define an activity group. For instance, Dragos correlates activity into groups based on similar behavior for the purposes of deriving more effective defensive strategies. If the activity in the group happens to be the responsibility of multiple organizations, countries, individuals, etc. this has no bearing on the analysis or derived conclusions from our groups.

Associating Activity Groups

Many analysts associate like-activity-groups together based on commonalities such as shared infrastructure, capabilities, or similar behaviors. Many analysts arrange the names and their associations or equivalencies from different companies, governments, and sources in a spreadsheet commonly referred to as "Rosetta Stones." However, equating two or more disparate analytically-derived groups is a mistake because this method effectively makes a group out of groups without concerning whether the individual groups were created using the same fundamental principles, bias mitigation, practices, or to answer the same analytic questions. If they were not, then the new "group of groups" will be fundamentally incorrect.

Therefore, it is with warning and hesitation that analysts should proceed with any cross-naming correlation if not done by the original analysts involved.

Questions and Answers

Here are selected questions received during our webinar on the topic and my answer.

Q: Do you know if any entity or source that happens to be correlating activity groups across vendors that can be used as a point of reference?

A: There are some that exist but I do not recommend the practice as it lacks the necessary protections against the problems with the practice as outlined above.

Q: How do you plan on working with other security companies on standardizing the naming conventions for the AG, or do you plan on keeping this internal to Dragos?

A: I have, for good or ill, been responsible for almost a dozen naming schemes. I have also been involved in several "cross-naming cooperative schemes" – these went poorly and ended up failures. Therefore, at Dragos we use rare earth mineral names and point out associations with the activity described by others but won't standardize with other companies at this time.

Q: What are you most excited about in the coming 2 years?

A: The fact that defenders are getting strong more quickly than adversaries. Things still won't be easier but we're seeing a rise in defense as never before. I'm excited to see that come to fruition.

Q: Can you compare the diamond model to the MITRE ATT&CK tool, aside from the fact that ATT&CK if for the IT side of the house? They are working on something ICS-specific. How do they differ? Can they be used in conjunction?

A: Just like the Kill Chain, all three (Diamond Model, ATT&CK, and Kill Chain) are complementary. They each try to accomplish different things. The Diamond Model is a model of intrusion analysis. The Kill Chain proposes a phase-based approach to detection and mitigation. ATT&CK defines a taxonomy for cyber threat behaviors and processes. They can all be used together!

Q: Even if you don't group the actors by the same names, can you group the activity groups to ones that may be the same actors or interest?

A: This can be done and is a valid method of conducting activity grouping. However, few analysts have access to the data necessary for grouping threats by same actor or interest (namely: national intelligence organizations). For the rest of us, all attempts to group by same actor or interest is usually a "grasping at straws" exercise based on inference rather than direct evidence. Example: if I state the interests of a group are conclusively set on a few industries, I may be making that conclusion based on little data when in fact the whole set of data points to a very different interest – a fallacy in arguing the general from the specific, or selection bias.

This blog post is a companion to the webinar: Uncovering Threat Activity Groups for Intelligence-Driven Defense.

Threat Activity Groups – Dragos from **Dragos, Inc.**