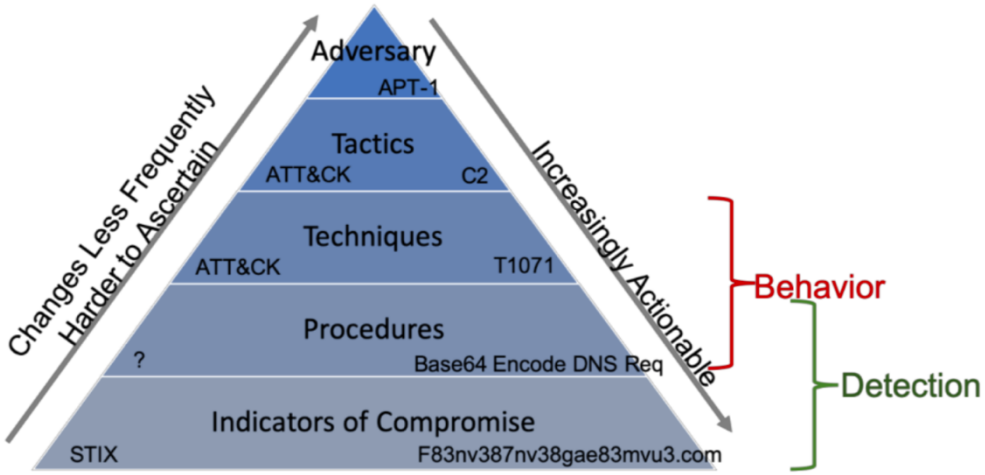
Beyond Indicator Sharing: Augmenting Adversary Playbooks with Behavior Objects

Cyber threat information sharing most often happens in one of two ways: (1) machine-readable Indicators of Compromise (IOCs) are shared using standardized languages and automated platforms; and (2) higher-level information is shared via blogs, vendor reports, and other labor-intensive processes. While IOCs can be shared quickly and consumed easily because they can be made machine-readable and machine-processible, attackers can easily change the IP addresses, URLs, e-mail addresses, and hashes described by these IOCs. Therefore, sharing and blocking IOCs is not sufficient to impose cost on the attackers and stop attacks. Unfortunately, the higher-level information about attacks shared in blogs and reports is not machine-readable, and thus it requires a great deal of time and effort for cyber defenders to extract and act upon the relevant information to stop attacks.

To improve information sharing, the cyber defense community needs to move beyond indicator sharing focused on detections of individual attacks, towards the sharing of machine-readable descriptions of attacker *behaviors* that span multiple attacks, as depicted in the figure below.



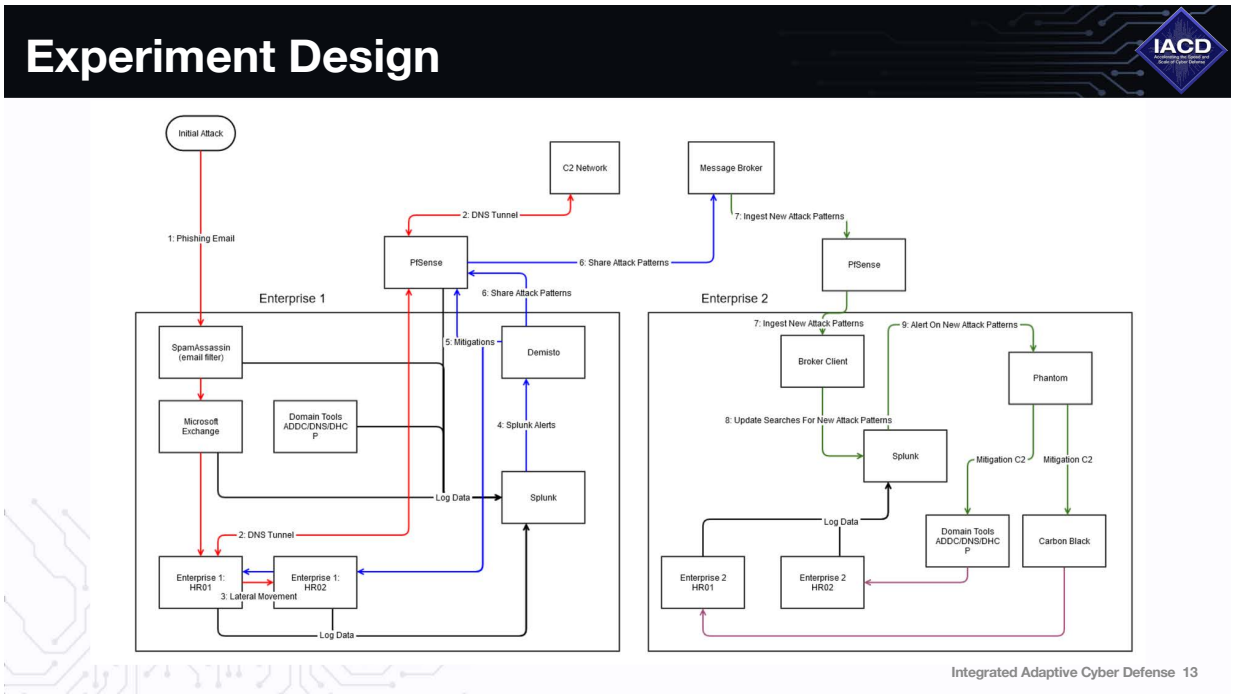
Integrated Adaptive Cyber Defense (IACD) has developed the concept of a "behavior object" to enable information sharing of actionable, machine-readable information regarding attackers activities across entire campaigns. A behavior object encapsulates detailed adversary tactics, techniques, and procedures (TTPs), providing actionable intelligence and enabling automated consumption and response. Behavior objects build upon concepts like Palo Alto's Unit42 adversary playbooks, which describe the TTPs that an adversary uses in a structured format (Palo Alto, 2017). Adversary playbooks use the STIX (Structured Threat Information Expression) language standard and MITRE's ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) knowledge base to represent adversary adversary tactics and techniques.

A behavior object extends an adversary playbook by providing more than just the tactics and techniques used by an attacker, identifying the patterns of affected machines across multiple attacks as well. The behavior object captures those sequences of attacker actions and ties them to alert triage and response options. It is this important extension to adversary playbooks – the ability to describe standard response actions to adversary attacks – that makes the behavior object valuable for information sharing via shareable automation workflows.

IACD conducted experimentation with an implementation of behavior objects to demonstrate actionable information sharing of attacker behaviors. The experiment showed how multiple attacks and executions of adversary playbooks can be encapsulated by a few behavior objects, and addressing those behavior objects with appropriate defenses and responses ends up countering a multitude of attacks.

In the experiment, IACD wrote detections for at least one technique within each of the ATT&CK tactic categories, using a Managed Detection and Response (MDR) tool from Defense Point Security. IACD used MITRE's Cyber Analytic Repository (CAR) to build from the behaviors to TTPs and associated analytics. In the experiment, depicted in the figure bleow, IACD demonstrated multiple benefits of the behavior object:

- detection of a multi-step attack involving a phishing e-mail compromise, command and control communication, and lateral movement (steps 1, 2, and 3)
- sharing of the detected attack pattern and mitigation to a second enterprise that used different security tools (step 6)
- automatic deployment of that attack pattern / mitigation within the second enterprise (step 7-9)



A behavior object enables information sharing of actionable threat intelligence, comprising both attacker action sequences and the defender responses to those actions. Successful sharing of behavior objects tied to response will enable mitigation of large numbers of attacks, disrupting the adversary kill chain.

For more information on behavior objects, actionable information sharing, and other experiments, please see the resources in the References section and visit https://www.iacdautomate.org.

References

[1] Palo Alto. (2017, December 15). Introducing the Adversary Playbook: First up, OilRig. Retrieved from Palo Alto: https://unit42.paloaltonetworks.com/unit42-introducing-the-adversary-playbook-first-up-oilrig/