Adversary Playbooks

An Approach to Disrupting Malicious Actors and Activity

PROTECT
DISRUPT
ELEVATE

CYBER THREAT ALLIANCE

POWERED BY CTA

Overview

Applying consistent principles to Adversary Playbooks in order to disrupt malicious actors more systematically.

Behind every cyber intrusion or attack is a human or group of humans. These threat actors, regardless of their motivation (e.g., warfare, espionage, crime, hacktivism, mischief, terrorism, or information operations), have a goal and they must successfully negotiate a series of steps to complete their mission. These steps can be depicted in logical sequences, such as the Lockheed Martin Kill Chain.[1] The complete collection of tools, techniques, and steps that adversaries use to achieve their goal, arrayed in that logical sequence, is the adversary's attack playbook.

If the cybersecurity community and network defenders have access to these playbooks, they can make their defensive activities more effective and impose increased costs on our adversaries. To that end, Cyber Threat Alliance (CTA) members share actionable intelligence that can be used to create such Adversary Playbooks. Further, since our cyber adversaries adapt very rapidly, CTA also automates the sharing and updating of this actionable intelligence.

While Adversary Playbooks can vary in scope, format, and depth, CTA believes that certain structures, elements, and features should be common across playbooks, so that readers have a consistent baseline from which to compare. This consistent framework would also enable cross-playbook analysis to identify broader threat indicators and adversary choke points. Therefore, this paper lays out a set of best practices for developing playbooks that would enable that commonality and facilitate ecosystem-wide analysis.[2] CTA's goal is not to set a standard, but rather to better inform the development of playbooks for the purposes of increasing our collective ability to address cyber threats.

CTA's Strategic Approach

CTA facilitates the sharing of cyber threat intelligence to improve defenses, advance the security of critical infrastructure, and increase the security, integrity, and availability of IT systems.

We take a three-pronged approach to this mission:

Protect End-Users
Our automated platform empowers members to share, validate, and deploy actionable threat intelligence to their customers in near-real time.

Disrupt Malicious Actors
We share threat intelligence to reduce the effectiveness of malicious actors' tools and infrastructure.

Elevate Overall Security
We share intelligence to improve our members' abilities to respond to cyber incidents and increase end-users' resilience.

This white paper provides details on one type of analysis, Adversary Playbooks, that supports this three-pronged approach.

[1] https://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html

[2] Due to variations in business models, not all CTA members will choose to publish playbooks.

Purpose

Adversary Playbooks are a tool that can help disrupt malicious cyber actors more effectively.

Cybersecurity cannot be approached with a "castle and moat" mindset, where we focus on keeping the bad guys "out" all the time. The network equivalent of walls and moats are necessary, but they cannot be the sole focus of network defense. In this mindset, we only have one chance to stop an intrusion, but no matter how high or thick our walls, or how wide and deep our moat, adversaries will inevitably find a way to get in if they try long enough. As a result, this approach ultimately fails.

Instead, we must shift to a strategy that gives defenders multiple opportunities to disrupt the adversary. The development and use of Adversary Playbooks can help identify these opportunities and illuminate the most effective defensive actions. This mindset focuses not on keeping the bad guys "out," but rather on preventing them from achieving their goal.

Target Audiences

Adversary Playbooks should be written at different levels of complexity for network defenders at cybersecurity providers versus for network defenders at end-user organizations.

Depending on where they work, network defenders require different levels of complexity and information regarding Adversary Playbooks. For example, network defenders at companies that provide cybersecurity services, such as cybersecurity vendors, cloud service providers, software makers, and telecommunications companies and ISPs, are often in the best position to leverage technical indicators and include them in their products to protect their customers. This group includes CTA members that actively share threat intelligence and choose to produce Adversary Playbooks, which can be leveraged on behalf of their customers.

Conversely, Adversary Playbooks should also be written for network defenders at end-user organizations, such as company Chief Information Security Officers (CISOs) and Security Operation Center managers. These network defenders maintain the systems they own and operate, including the provisioning of security patches and updates. These actions are integral to disrupting adversary activity but are not typically controlled by cybersecurity providers. Except for very sophisticated end-users, receiving technical indicators may not be as useful to this second group, but knowing what specific mitigation recommendations they should take within their own enterprise would provide additional opportunities for disrupting adversaries across the Kill Chain. These playbooks would also include Executive Summaries for Chief Executive Officers (CEOs) and Boards, focusing on risk management and potential impacts around the specific threat to help motivate mitigations and prioritize activity.

Structure of Adversary Playbooks

Adversary Playbooks should, at a minimum, describe the tools adversaries often employ; the tactics, techniques, and procedures they frequently use; and the typical ways adversaries employ those tools to achieve their goals.

Topics

Adversary Playbooks can be developed for a wide variety of **actors**, **activities**, **and targets**, over a specific **timeframe or campaign**. Examples of Adversary Playbooks could include the following:

- Named actor sets (e.g., Oil Rig, Sofacy) and incidents that target certain sectors;
- Ransomware against any organization;
- Nation-state espionage campaigns against Defense Industrial Base companies; and
- Intellectual Property theft from manufacturers.

Core Elements

Adversary Playbooks should contain certain core elements that will enable comparability and cross-playbook analysis. These core elements include the following:

1. **Technical Profile** – describes:
    - the specific adversary, a generic adversary type, or the generic effect an adversary wants to achieve, along with
    - the tools and tactics, techniques, and procedures (TTPs) typically associated with the adversary or effect.
2. **Typical Plays** – demonstrates how the adversary typically employs those observables, capabilities, and TTPs in certain exemplar scenarios, through a collection of attack techniques defined by MITRE's Adversarial Tactics, Techniques & Common Knowledge (ATT&CK)[3] model and laid out according to the Kill Chain structure.
3. **Recommended Actions** – describes the defensive actions and mitigations that will have the greatest impact and return on investment, based on the profile and typical plays described in the first two elements.
4. **Technical Indicators** – provides a compilation of the technical indicators used to build the playbook in a shareable format via Structure Threat Information Expression (STIX)[4], which are also included in the CTA Platform prior to public release.

Formats

As discussed above, Adversary Playbooks should come in two different forms, based on the target audience:

Adversary Playbooks for End-Users	Adversary Playbooks for Cybersecurity Providers
✓ Consist of the first three elements: technical profile, typical plays, and recommended actions	✓ Consist of all four elements: technical profile, typical plays, recommended actions, and technical indictors
✓ Recommended actions focus on mitigations that network defenders can take within their organizations across the Kill Chain	✓ Identifies technical observables and indicators across the Kill Chain that members can use to protect their customers
✓ Include an Executive Summary for CEOs and Boards, focusing on risk management and potential impacts around the specific threat	✓ Recommended actions focus on activities these entities can take to protect their customers
✓ Available publicly	✓ Available publicly[5]
✓ May incorporate data and recommendations that combine information from multiple Adversary Playbooks for cybersecurity providers	

[3] https://attack.mitre.org/wiki/Main_Page

[4] https://oasis-open.github.io/cti-documentation/

[5] CTA members typically have access to the technical indicators associated with a playbook through the CTA's intelligence sharing platform.

Playbook Principles

In addition to a common structure, Adversary Playbooks should adhere to a common set of principles, which will help ensure a higher level of quality.

Adversary Playbooks Principles	

Provide context & action	- Describe the Threat, including:
	  ▪ the tools adversaries often employ
	  ▪ the tactics, techniques, and procedures they frequently use
	  ▪ the typical ways adversaries employ those tools to achieve their goals
	- Describe the impact if the threat materializes
	- Describe the mitigations to address these elements:
	  ▪ Tailor network defenses to disrupt malicious activity at multiple points along the Kill Chain simultaneously, strengthening systems and increasing the odds of success
	  ▪ Identify the points of greatest effectiveness where defensive actions can have the broadest possible effect

Not let the perfect be the enemy of the good	- We will never have a "complete" Adversary Playbook; we will always have holes - Playbooks should acknowledge this fact and actively seek additional data to fill in the holes through a regular update process

Ensure data quality via CART	- Completeness:
	  ▪ Provide enough detail for a proper response
	- Accuracy:
	  ▪ Ensure the data enables defenders to take the right actions
	- Relevance:
	  ▪ Address threats relevant to the target audience's business operations
	- Timeliness:
	  ▪ Produce and deliver quickly enough to make a difference
	  ▪ Maintain in an on-line repository, so that the technical indicators can receive automated updates from sources, such as the CTA Platform
	  ▪ Update regularly on longer time scales (e.g., every six months to annually) for elements other than the technical indicators

Be tailored	- Address specific risks and threats, and speak to specific audiences (e.g., cybersecurity providers, critical infrastructure sectors, governments, leadership within organizations, etc.) - Clearly identify the risks, threats, and audiences
Inform future data collection efforts	- Use data gaps to identify collection priorities for the CTA Platform
Respond to feedback from users	- Routinely ask for feedback (e.g., links to questionnaires, forms) and make changes to Adversary Playbooks based on the feedback received

What's Next

A few CTA members have produced initial versions of Adversary Playbooks in consideration of these principles. In the coming months, certain CTA members will publish additional Adversary Playbooks. Over time, these Playbooks will allow our members to more systemically disrupt malicious cyber activity on behalf of, and eventually hand-in-hand with, their customers. Additionally, CTA believes that over time, playbook development will be improved by diversifying membership, and thus data, within CTA. This data diversity includes companies with visibility into threats to various information and communications technology systems, such as endpoint devices, network infrastructure, mobile devices, and ICS/SCADA systems, or threats that vary geographically.

About the Cyber Threat Alliance

The Cyber Threat Alliance (CTA) is the industry's first formally organized group of cybersecurity practitioners that work together in good faith to share threat information and improve global defenses against advanced cyber adversaries. CTA's mission is to facilitate the sharing of actionable intelligence and situational awareness about sophisticated cyber threats to improve its members' cyber defenses, more effectively disrupt malicious cyber actors around the world and raise the level of cybersecurity throughout the Internet and cyberspace. The alliance is continuing to grow on a global basis, enriching both the quantity and quality of the information that is being shared across the platform. CTA is actively recruiting additional regional players to enhance information sharing to enable a more secure future for all.

For more information about the Cyber Threat Alliance, please visit: http://cyberthreatalliance.org.

Cyber Threat Alliance
1001 19th St. N., Suite 1200
Arlington, VA 22209
feedback@cyberthreatalliance.org
https://www.cyberthreatalliance.org

PROTECT
DISRUPT
ELEVATE