Decider

A Tool for Network Defenders, Analysts, and Researchers Working With MITRE ATT&CK®

March 2023

OVERVIEW

On March 1, 2023, CISA released Decider, a tool for mapping adversary behavior to the MITRE ATT&CK® framework. A companion to the recently updated Best Practices for MITRE ATT&CK® Mapping guide, Decider helps network defenders, analysts, and researchers quickly and accurately map adversary tactics, techniques, and procedures (TTPs) to the ATT&CK knowledge base.

MITRE ATT&CK is a publicly available knowledge base of adversary tactics and techniques based on real-world observations. ATT&CK has been adopted by CISA and network defenders worldwide because it helps cyber threat intelligence (CTI) analysts and others understand adversary behaviors.

At the same time, the process of using ATT&CK can be challenging. Mapping different forms of observable data to ATT&CK techniques requires understanding both the behavior itself as well as ATT&CK.

CISA is releasing the Decider tool to help the community use ATT&CK more efficiently and effectively. CISA created Decider and the best practices guide in partnership with the Homeland Security Systems Engineering and Development Institute™ (HSSEDI) and the MITRE ATT&CK team.[1]

WHY DECIDER?

Since the original publication of the best practices guide in June 2021, CISA has found that while ATT&CK is a valuable tool for enterprise cybersecurity, there are many intricacies in creating ATT&CK mappings that are important to get right and easy to get wrong.

Decider makes creating ATT&CK mappings easier to get right by walking users through the mapping process. It does so by asking a series of guided questions about adversary activity to help users arrive at the correct tactic, technique, or subtechnique. Decider has a powerful search and filter functionality that enables users to focus on the parts of ATT&CK that are relevant to their analysis. Decider also has a cart functionality that lets users export results to commonly used formats, such as tables and ATT&CK Navigator™ heatmaps.

By making ATT&CK mapping easier, Decider helps users more quickly and accurately understand adversary activities. After obtaining accurate mappings, users can move on to many other ATT&CK activities, including:

- Visualizing the findings in ATT&CK Navigator
- Sharing the findings with others by publishing threat intelligence reports
- Finding sensors and analytics to detect those techniques
- Discovering mitigations that help prevent techniques from working in the first place
- Compiling threat emulation plans to validate defenses

[1] HSSEDI is a DHS-owned federally funded research and development center (FFRDC) that is managed and operated by The MITRE Corporation.

USING DECIDER

Note: Decider is a web application that must be hosted before it can be used. See the bottom section of this document for information on getting an instance running in your environment.

In the main workflow, Decider will ask a series of questions about the adversary activity to be mapped using straightforward language (see figure 1). Answering those questions will drill down into tactics, techniques, and subtechniques until a mapping is reached.

For example, the first question is "What is the adversary trying to do?" One possible answer is "**Gaining an initial foothold** within the victim environment," which corresponds to the Initial Access tactic. Clicking that answer will then present you with a question about how the adversary tried to achieve that initial foothold.

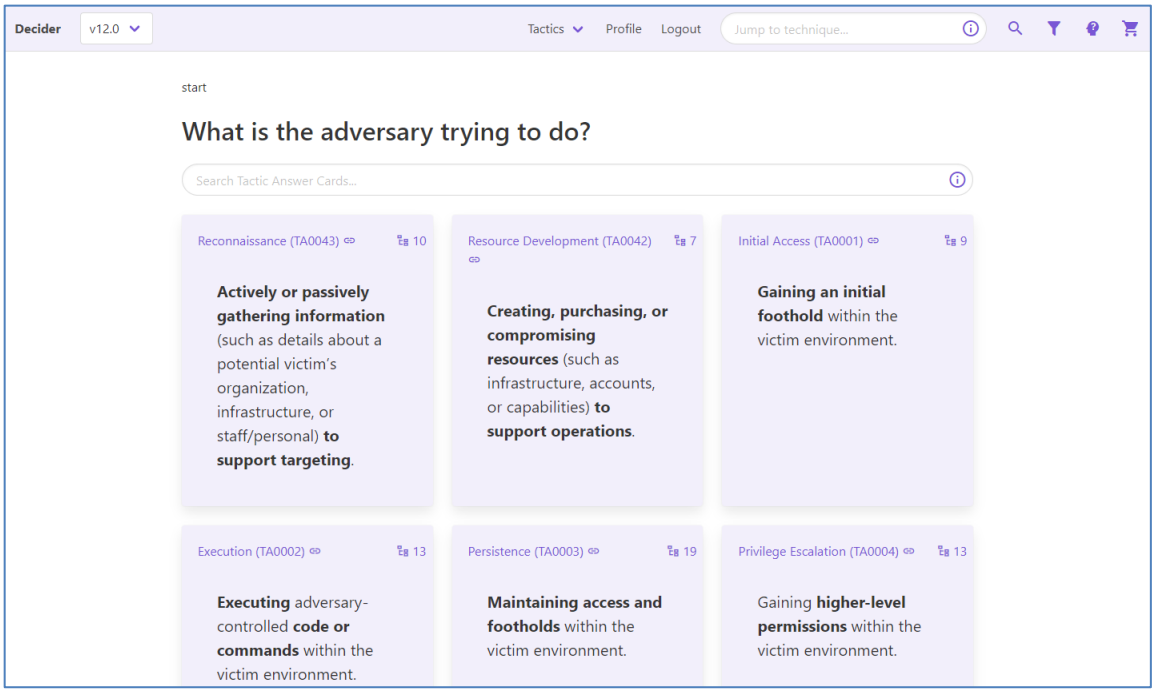

Figure 1: Mapping to ATT&CK by answering questions

Decider will continue to ask questions about the activity until you reach a subtechnique or, if no subtechnique fits, a technique. Decider presents information to help you confirm the mapping, including information about the technique directly from MITRE ATT&CK, similar techniques, and potentially incorrect mappings.

You can also save the (sub)technique in your cart (see figure 2) along with notes on the observation or usage of the technique. You can save and export your cart as a JavaScript Object Notation (JSON) file (for uploading to Decider or processing with scripts), an ATT&CK Navigator layer, or a Microsoft Word table.

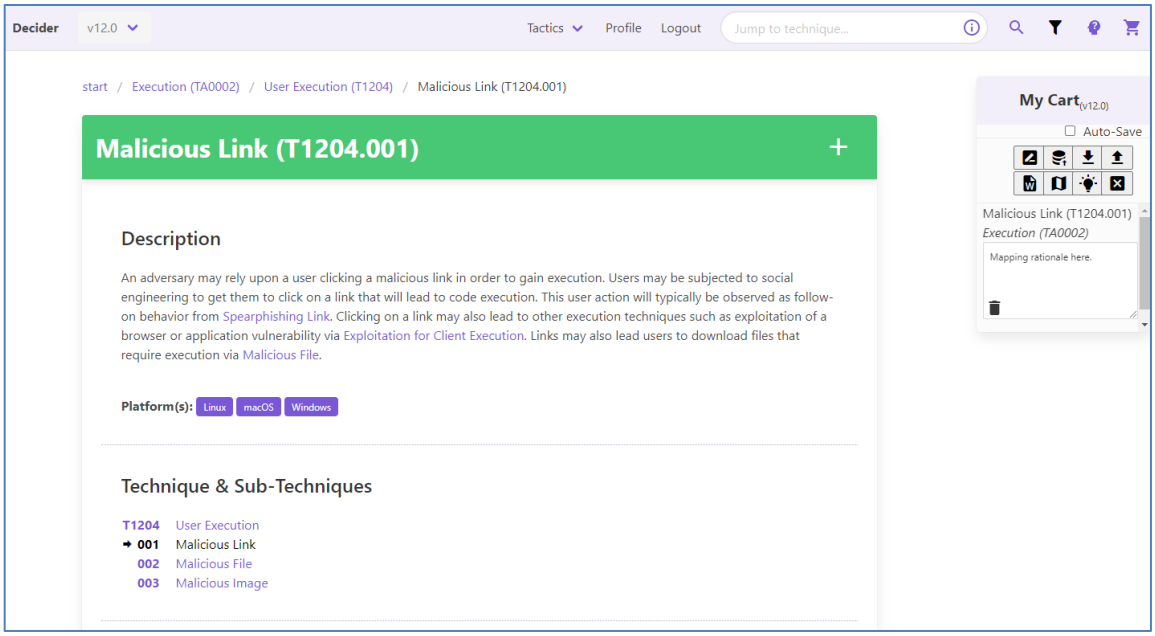

Figure 2: Subtechnique landing page and cart

Decider's search allows users to jump straight to a technique or subtechnique, which is helpful when the main workflow does not deliver the correct technique or when the user has already identified the technique or subtechnique used.

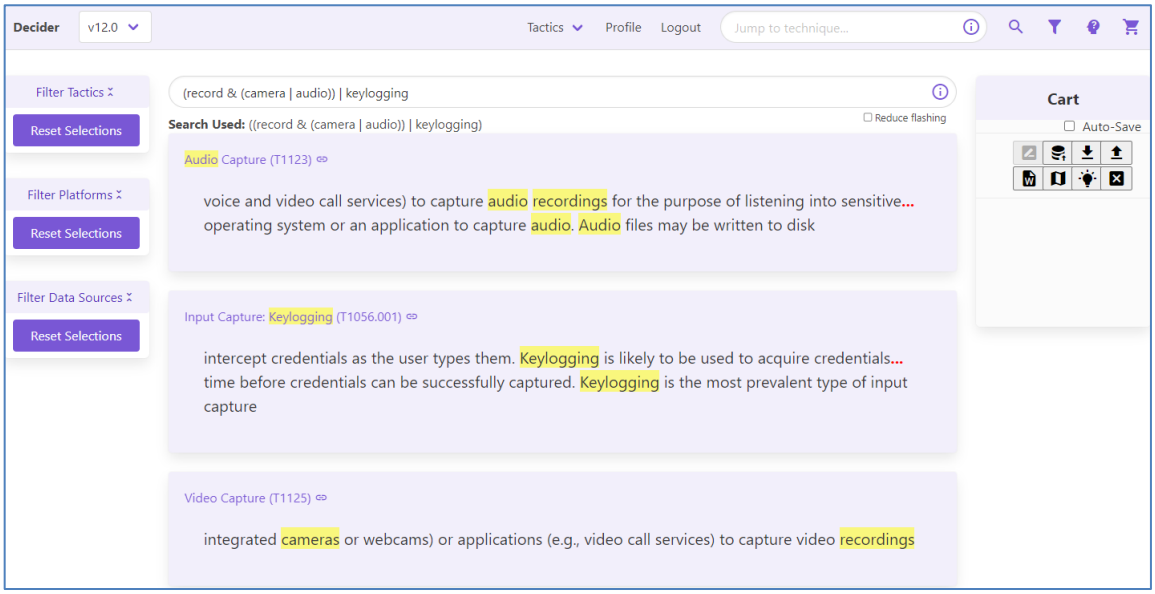

Figure 3: Search function example

HOSTING AND CUSTOMIZING DECIDER

Decider is a web application that must be hosted to be used. Organizations can host Decider internally to save and share customized mismappings, questions, answers, and users per install.

CISA does not offer access to a running instance of Decider. Decider is currently compatible with Enterprise

ATT&CK versions 11.0 and 12.0. The in-app version selector allows users to switch between installed versions.

DOWNLOAD

Please visit the CISA GitHub site to download Decider. Submit feedback, bug reports, and feature suggestions by opening an issue on the GitHub page.

For more on identifying and countering adversary behavior, see Best Practices for MITRE ATT&CK® Mapping and CISA's Shields Up resources.