

USING THE MITRE ATT&CK FRAMEWORK TO ANALYZE THREAT ACTORS & MALWARE

Mandiant Advantage Threat Intelligence (MATI) allows you to explore Threat Actors and Malware on the basis of the **MITRE ATT&CK® Framework** (<https://attack.mitre.org/>). Analyzing Threat Actors and Malware this way helps you explore threats in terms of adversary Tactics, Techniques, and Procedures (TTPs) based on real-world observations.

In the MITRE ATT&CK Framework:

- **Tactics** (<https://attack.mitre.org/tactics/enterprise/>) represent the route or path of a MITRE ATT&CK technique or sub-technique, which is the tactical goal (*why*) of an adversary.
- **Techniques and sub-techniques** (<https://attack.mitre.org/techniques/enterprise/>) represent *how* an adversary achieves a tactical goal by performing an action.



MATI currently supports MITRE ATT&CK version 8 (v8).

After reading this article, you will be able to:

- **Discover how to analyze Threat Actors and their associated TTPs** by focusing on use cases for tightening your security controls throughout the attack lifecycle.
- **Test your defenses against specific Malware or Threat Actors** directly in the Mandiant Security Validation (MSV) platform if you have a subscription.
- **Learn how to explore specific Malware families**, using the role of Backdoor as an example filter.

Video: Explore MITRE ATT&CK

Analyze Threat Actors using the Explore MITRE ATT&CK Dashboard

For example, say you want to explore the TTPs associated with five Actors recently observed targeting the automotive industry:

- UNC2500
- UNC2633
- UNC2824
- UNC4705
- UNC2529

To filter and analyze Threat Actors

1. Select **Explore > MITRE ATT&CK** to go to the Explore MITRE ATT&CK dashboard
2. Choose **Actors** from the drop-down. This displays all Actors currently tracked by Mandiant.
3. Select **Automotive** from the list of **TARGET INDUSTRY** filters to narrow your search.
4. Sort the resulting **Actors List** by **Last Seen - Most Recent**.

The screenshot shows the 'Explore MITRE ATT&CK' interface with the 'Actors' tab selected. At the top, there are buttons for 'Actor Selection' and 'Analysis'. Below this, a list of selected actors is displayed, including TEMP.Armageddon, UNC3313, UNC4992, UNC5112, UNC4221, UNC3319, UNC2093, UNC4984, UNC5439, UNC4536, UNC5055, APT44, UNC5296, UNC1151, UNC1543, FIN8, UNC2165, and UNC5176. A search bar and filters are on the left. The main area shows a grid of threat actor cards, each with a name (e.g., UNC2500, UNC2824, UNC4393, UNC1069), a brief description, and various filters for source region, target industry, and target countries.

5. Click **Analysis** or **Next** to populate the MITRE ATT&CK heat map with TTPs specific to the **Selected Actors**.

The screenshot shows the 'Analysis' tab of the 'Explore MITRE ATT&CK' interface. The 'Selected Actors' list is the same as in the previous screenshot. Below the list, a 'MITRE ATTACK' section displays a heat map of techniques. The techniques are grouped into categories: Reconnaissance (3 techniques), Resource Development (4 techniques), Initial Access (9 techniques), Execution (8 techniques), Persistence (13 techniques), Privilege Escalation (11 techniques), Defense Evasion (24 techniques), and Credential (11 techniques). Each technique is represented by a colored square with a count, indicating the number of selected actors associated with that technique. For example, 'Command and Scripting Interpreter' has a count of 18, and 'Abuse Elevation Control Mechanism' has a count of 5.

If more than one Actor is selected and analyzed as per the MITRE ATT&CK framework, the heat map shows the number of selected Actors associated with each technique or sub-technique to aid in prioritizing mitigation efforts. If there are multiple sub-techniques associated with a technique, an expander arrow can be clicked to reveal them. Clicking directly on either a technique or a sub-technique provides a brief description.

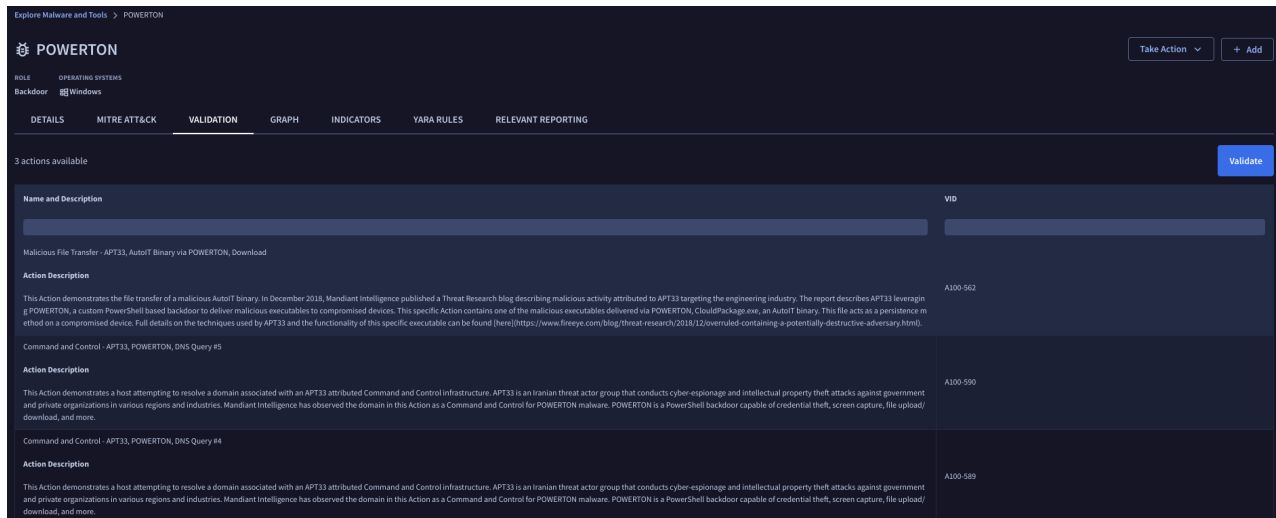
You can select and de-select **Actors** on the heat map page itself to easily compare Actor TTPs within the heat map view.

Testing defenses against Threat Actors

If you have a Security Validation subscription, selecting either a technique or a sub-technique also provides a list of Actions that can be used in the Security Validation platform to test your defenses against it. Click the expander arrow (>) to review the description of each Action.

You can only view **Validations** if you have a Security Validation subscription.

Click **Validate** to pivot directly to the Security Validation platform and test your defenses.



Download the MITRE ATT&CK heat map as a CSV

You can download the MITRE ATT&CK (multi-actor) heat map as a CSV file for further analysis by clicking [Download TTPs](#). This allows you to filter and sort heat map data to aid in prioritizing mitigation efforts. For example, you can filter on specific techniques or sub-techniques for a given MITRE Category Name (or, tactic), and then sort Actor(s) Usage Count to focus on the most commonly used techniques.

The following fields are included in the exported CSV file:



- MITRE Category Name
- Technique ID
- Technique Name
- Sub-Technique IDs
- Sub-Technique Names
- Actor(s) usage count
- Actor 1
- Actor 2
- Actor 3

Analyze Malware using the Explore MITRE ATT&CK Dashboard

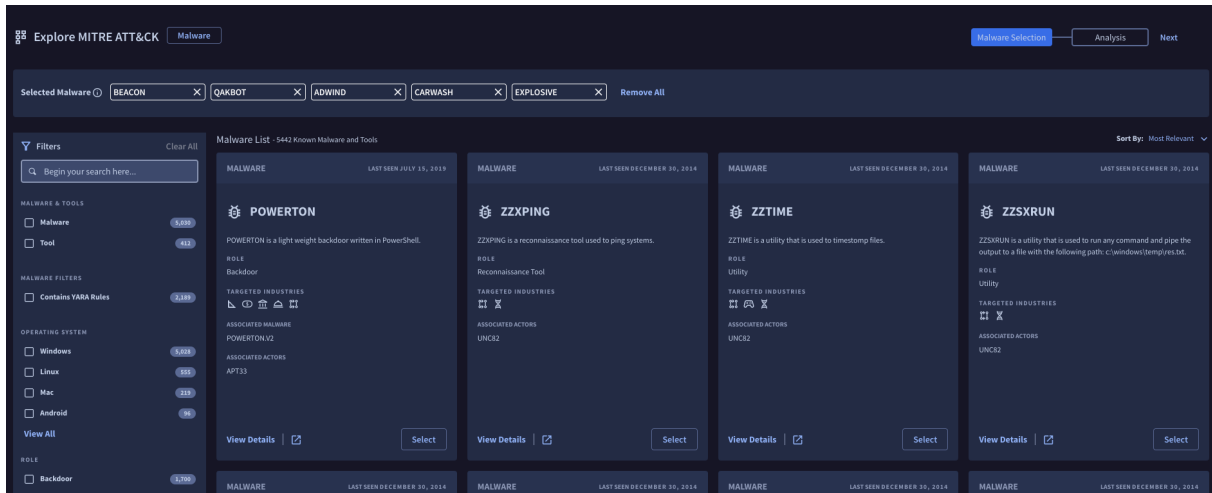
The workflow for exploring Malware is similar to exploring Actors, but with different filtering options. For example, suppose a recent report noted an increased use of backdoor Malware in your industry. A vulnerability scan of Malware in your environment included the following Malware families, so you want to explore them further to understand your associated risk:

- BEACON
- QAKBOT
- ADWIND
- CARWASH
- EXPLOSIVE

To filter and analyze malware

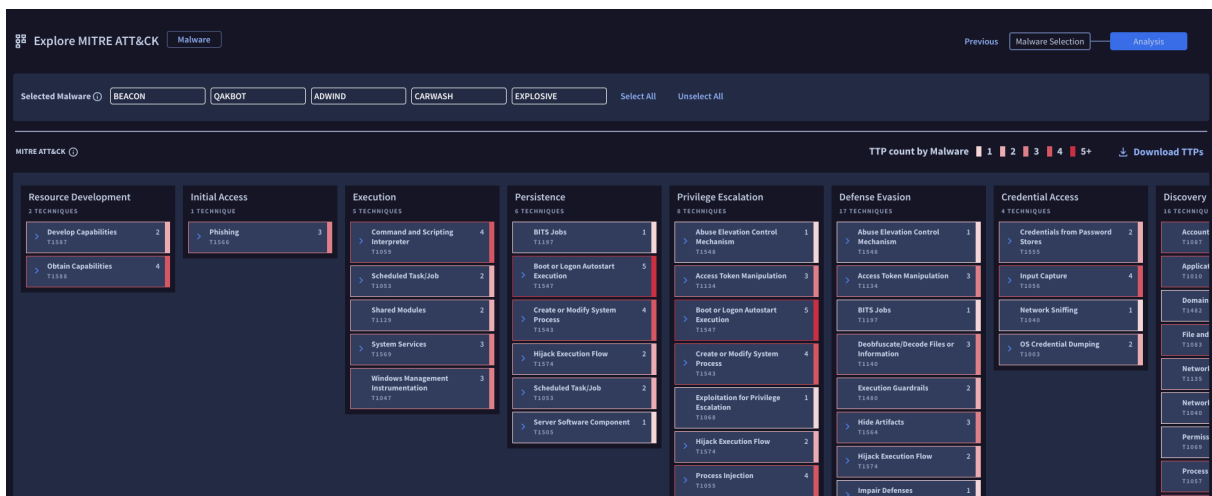
1. Select **Explore > MITRE ATT&CK** to go to the Explore MITRE ATT&CK dashboard
2. Choose **Malware** from the drop-down.

3. Select **Backdoor** from the list of **ROLE** filters.
4. Select the five Malware families noted in your vulnerability scan.




The screenshot shows the 'Explore MITRE ATT&CK' interface. At the top, there are buttons for 'Malware Selection', 'Analysis', and 'Next'. Below this, a 'Selected Malware' list contains: BEACON, QAKBOT, ADWIND, CARWASH, and EXPLOSIVE. A 'Filters' sidebar on the left shows 'Malware' and 'Tool' selected, and 'Backdoor' selected under the 'ROLE' section. The main area displays details for five malware families: POWERTON, ZZXPING, ZZTIME, and ZZSXRUN. Each family card shows its name, role, targeted industries, and associated actors.

5. Click **Analysis** or **Next** to populate the MITRE ATT&CK heat map with TTPs specific to the selected Malware.



The screenshot shows the 'Explore MITRE ATT&CK' interface with the 'Analysis' button selected. The 'Selected Malware' list remains the same. The main area displays a 'TTP count by Malware' heat map. The heat map is organized into columns for different categories: Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, and Discovery. Each category contains a list of techniques and sub-techniques with their respective counts. For example, under 'Execution', 'Command and Scripting Interpreter' has a count of 4, and 'Scheduled Task/Job' has a count of 2. Under 'Persistence', 'BITS Jobs' has a count of 1, and 'Boot or Logon Autostart Execution' has a count of 5. Under 'Privilege Escalation', 'Abuse Elevation Control Mechanism' has a count of 1, and 'Access Token Manipulation' has a count of 3. Under 'Defense Evasion', 'Abuse Elevation Control Mechanism' has a count of 1, and 'Access Token Manipulation' has a count of 3. Under 'Credential Access', 'Credentials from Password Stores' has a count of 2, and 'Input Capture' has a count of 4. Under 'Discovery', 'Account' has a count of 1, and 'Domain' has a count of 1.

 You can select and de-select **Malware** on the heat map page itself to easily compare **Malware** TTPs within the heat map view.

If more than one Malware is selected and analyzed in the MITRE ATT&CK framework, a heat map displays the number of selected Malware associated with each technique or sub-technique. As with Threat Actors, if you have a subscription to Security Validation and you click on a technique or sub-technique, you can pivot directly to the Security Validation platform to test your defenses against it. Again, you can download the heat map as a CSV for further analysis to aid in prioritizing mitigation efforts against the selected Malware.