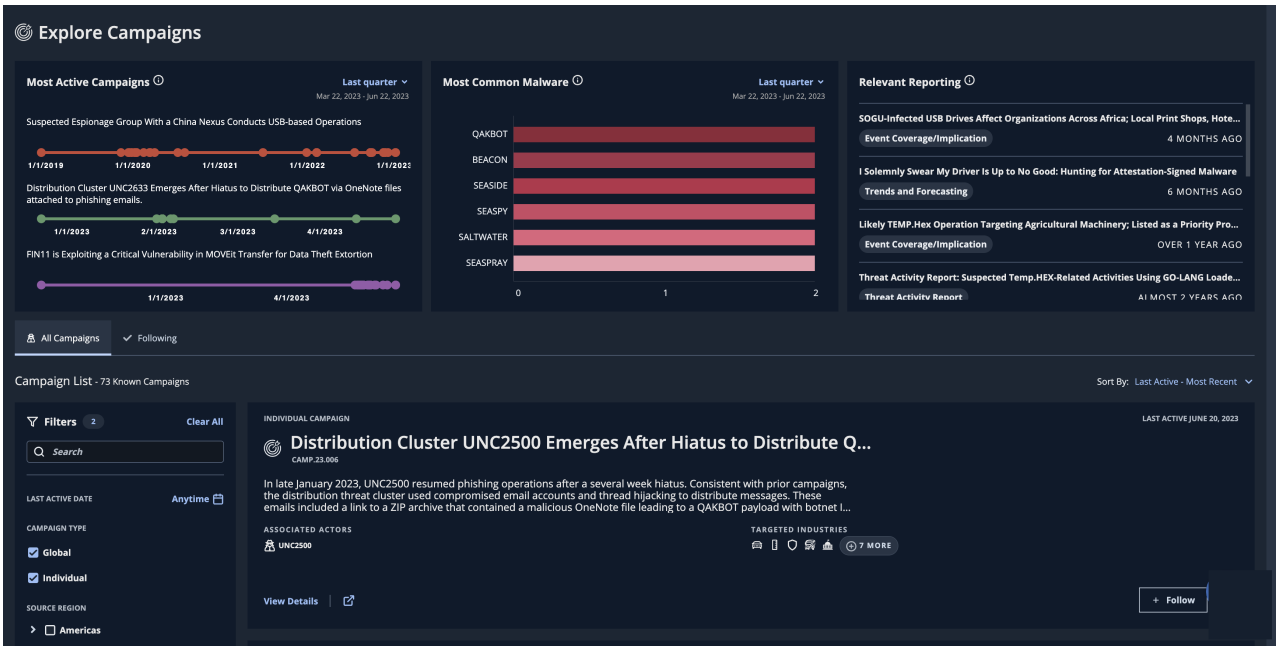
THREAT CAMPAIGNS

Security teams may struggle with understanding their threat landscape and determining what activity to focus on, especially when faced with a myriad of emerging threats. To better assist these teams, the Threat Campaign feature in Mandiant Advantage Threat Intelligence (MATI) gives security professionals visibility into active campaigns affecting their industries, regions, and peers.

This feature provides a campaign-centric view and lets you easily pivot across all accompanying intelligence. Campaigns help you better prioritize mitigation and response actions in preparation for the next attack with a high degree of confidence. Data is updated daily as analysts get new campaign details, so you get access to Mandiant's knowledge in near real-time.



This video provides an overview of Threat Campaigns.

Campaign Creation

Mandiant analyzes emerging threat data directly from client engagements and from open source or other collections methods when assessing a campaign's viability for a Threat Campaign profile. Considerations for campaign creation include the following:

- Who is the threat actor, what are their motivations, and how impactful are their operations on targeted organizations? For example, an espionage actor targeting Ministries of Foreign Affairs or a fast-paced extortion operator does not equate to automated drive-by adware or infostealer campaigns.
- What level of insight into the campaign do we have? Can we confirm that multiple organizations have been targeted? Do we have a sufficient amount of shareable, actionable data that we can disseminate to our clients?
- Is the targeting broad enough that the targeted organizations could not be discerned based on the data we have available to share?

> We take sensitivities of this data very seriously and make every effort to restrict the unintended release of sensitive, client-attributable data into the Threat Campaign profile.

Campaign Types

There are two types of campaigns that are reported in MATI:

- **Individual Threat Campaign**: These campaigns are created when an actor or multiple actors cooperate toward a single objective at multiple targets within a relevant time period.
- **Global Threat Campaign**: These campaigns are created when multiple unrelated actors run parallel campaigns involving a similar theme, target, or resource. A common example is multiple threat actors starting campaigns that exploit a recently released zero-day vulnerability.

Campaign Features

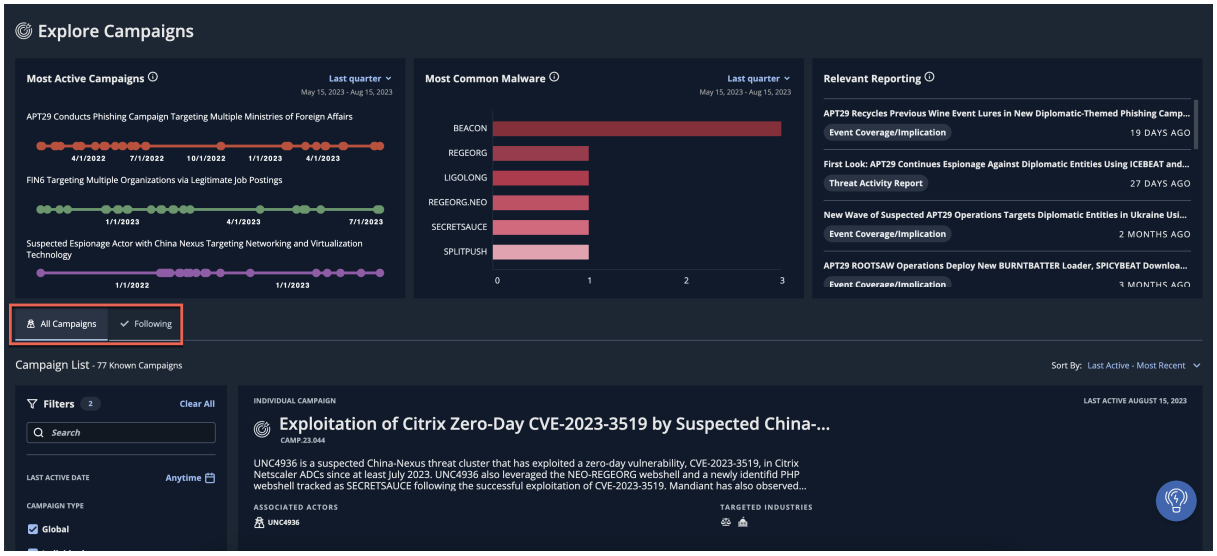
Campaigns provide the following features:

- **Dashboards**: At-a-glance dashboards provide a view of the most active campaigns and most commonly observed malware across all campaigns for a given time period.
- **Campaign List**: A list of the latest reported individual and global actor campaigns. You can use various filters to pare down the list: Campaign Type, Source Region, Target Industry, and Target Region.
- **Campaign Details**: A summary of campaign details is automatically updated as new events are observed. This includes a high-level timeline of events, targeted industries and regions, and associated malware and vulnerabilities.
- **Campaign Timeline**: A detailed timeline of observed attacker techniques and analyst identified "key events" provides context on the sequence and importance of observed attacker activities during a campaign.
- **Example Attacker Techniques**: Actual examples of commands executed by the attacker and evidence of attacker activity in event logs lets you see what our analysts see during the campaign.

Follow Campaigns

In the **All Campaigns** tab, click **Follow** for any Campaign to monitor changes to the selected Campaigns over time, such as new activity, associations, or reporting.

- Navigate to the **Following** tab to view all the Campaigns being followed.



Filter Most Active Campaigns and Most Common Malware

The following dashboards are available on the **Explore Campaigns** page.

- **Most Active Campaigns**: Campaigns with the most activity during the selected timeframe. Activity is measured by the number of events on the campaign timeline.
- **Most Common Malware**: The most common malware families across all campaigns during the specified

timeframe. For example, if the malware family BEACON was observed across seven campaigns during the selected timeframe, the total count for BEACON would be 7.

- **Relevant Reporting**: Intelligence reporting related to the most active campaigns during the selected time period

By default, the Most Active Campaigns and Malware dashboards on the Explore Campaigns page show timeline data from the last quarter. You can change this view to suit your needs.

1. Go to **Explore** > **Campaigns**.
2. From either dashboard, click the down arrow .
3. (Optional) If desired, click the drop-down and change the value from **quarters** to another time range: **days**, **weeks**, or **months**.
4. Enter a different numeric value to change the historical range of data (for example, two days, weeks, months, or quarters).

View Campaign Details

All active campaigns, both individual and global, appear in full in the Campaign List. You can search or filter on the results and open a specific campaign to access its more granular details. Campaigns are automatically updated as analysts tag events.

1. Go to **Explore** > **Campaigns**.
2. (Optional) Use the search bar or filters, as needed, to narrow down the list of campaigns.
3. Click the campaign headline to open the campaign details.
4. (Optional) Move the sliders to narrow down or expand the time range of the Campaign Timeline, as needed.
5. Review the summary details, which provide information about the campaign itself, such as timeline, associated actors, and targeted industries.

> Some campaigns are part of a larger (global) campaign. These campaigns also include associated campaigns in the details view. You can click those campaign links and go to the detail view for the individual campaigns. The associations that may also appear are related actors, related malware families, and operations or externally named campaigns.

6. To view more specific information about the MITRE ATT&ACK framework, timeline/techniques, and indicators, click **View Full Link**. This page also has the campaign details in the **Details** tab.

> Click to open the full link in a new tab. This method makes it easier to return to your previous view when you're finished reviewing the full details about the campaign.

The full link appears with multiple tabs that you can click for more information about the campaign.

- Click **MITRE ATT&CK** for a summary of adversarial Tactics, Techniques, and Procedures (TTPs) from the MITRE ATT&CK framework that have been observed in the campaign.
  - All TTPs associated with the campaign can be downloaded by clicking **Download TTPs** from the **Actions** drop-down.

- Click **Timeline** to access the following:
  - A more detailed view of the timeline for the campaign. For more details, see **Mandiant Techniques (https://docs.mandiant.com/home/mandiant-techniques)**.
  - A list of Mandiant techniques, which are part of our internal taxonomy for classifying attacker activity. For more details, see **Mandiant Techniques (https://docs.mandiant.com/home/mandiant-techniques)**.
  - A list of relevant events that were identified as a pivotal component of the campaign
  - A list of host commands, which are significant commands issued by an attacker during the campaign

- A list of malicious executables compiled, which are relevant time events for malicious executables used in this campaign

- Click **Indicators** to access indicators that are associated with the campaign. See **Indicators (https://docs.mandiant.com/home/indicators)** for more information.

  The following fields are included in the exported CSV file when you download indicators:
  - Indicator Value
  - Indicator Type
  - IC Score
  - Associated Actors
  - Associated Malware
  - Associated Tools
  - Associated Campaigns
  - Exclusive
  - First Seen
  - Last Seen

  - All indicators associated with the campaign can be downloaded by clicking **Download Indicators** from the **Actions** drop-down.

- Click **Relevant Reporting** to view the latest finished intelligence reports that are related to or explicitly mention the campaign.