Mandiant

MANDIANT TECHNIQUES AND KEY EVENTS ON THE TIMELINE

The timeline consists of the following events related to campaigns:

- **Mandiant Techniques**: Direct observation of an attacker using an identified Mandiant attacker methodology during the campaign. A direct observation for these purposes is defined as the issuance of host commands or the identification of host-based events that provide evidence of this attacker executing this technique. The inclusion of Mandiant techniques, coupled with the example techniques, is designed to provide actionable detail on observed actor activity during the campaign.
- **Event**: Event identified by an analyst as a pivotal component of a campaign. These can include external events, like the date an exploit for a vulnerability was identified or the date a patch for that vulnerability was made available, or evidence of significant attacker activity identified in event logs during the campaign.
- **Host command**: Significant command issued by an attacker during a campaign. These commands may include things like an attacker launching a malicious executable, saving files to disk, or targeting sensitive data.
- **Malicious Executables Compiled**: Dates of malicious executables compiled that align with the campaign's activity. This may illustrate, for example, that an attacker compiled their malicious binaries days before or targeting an organization or perhaps, they compiled them while the attack was in progress.
- **X509**: Creation of a key X509 certificate used during a campaign, such as SSL certificates. This gives insight into an attacker's command and control operations.
- **Phishing email**: A phishing email event significant to a campaign. This may include dates of identified phishing waves, including those identified to be the initial infection vector during the targeting of an organization.

Mapping Mandiant Techniques to MITRE ATT&CK

Mandiant Techniques are part of our internal taxonomy for classifying attacker activity. As first responders to hundreds of global security incidents across government and commercial industries, we have direct insight into attacker methodologies and capabilities. Our analysts create new Mandiant techniques as we observe attackers using new methodologies to target victim organizations. This allows us to categorize attacker activity at the time of observation and removes any reliance on categorization by external organizations. Our detailed catalog of attacker techniques helps us better detect, attribute, and respond to a wide variety of attackers.

Mandiant maps its findings to the MITRE ATT&CK framework. While there are many similarities between techniques in both models, Mandiant techniques often provide a more granular view into attacker activity. This level of granularity enables our own threat intelligence and incident response efforts.

For example, the Mandiant technique may specify the specific type of exploit observed (for example, SQL injection), as opposed to the more generic MITRE technique for "Exploit Public Facing Application."

Key Events

The timeline overview also shows several types of key events that are relevant to the campaign, as tagged by analysts – for example, host commands that were executed by the threat actor and the compile times of malicious executables. Where possible, actual examples of host commands and evidence of attacker activity that illustrate the attacker's tactics, techniques, and procedures (TTPs) are provided to assist organizations with their detection and mitigation efforts. The events give you a view of what Mandiant analysts are seeing.

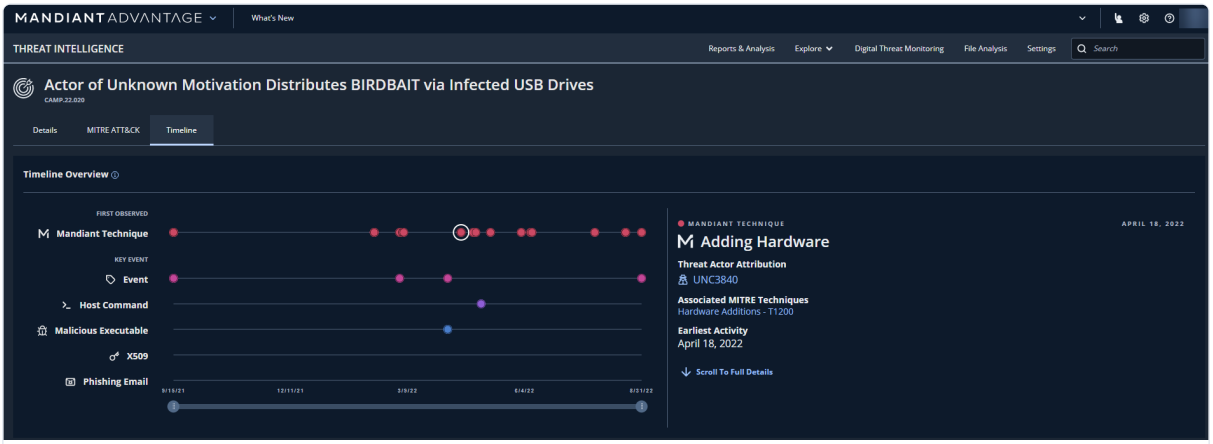
Not all components may be available for a specific campaign, but if analysts tagged them, you'll see them in the timeline view.

To Access Mandiant Techniques

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, and then click **View Full Link**.

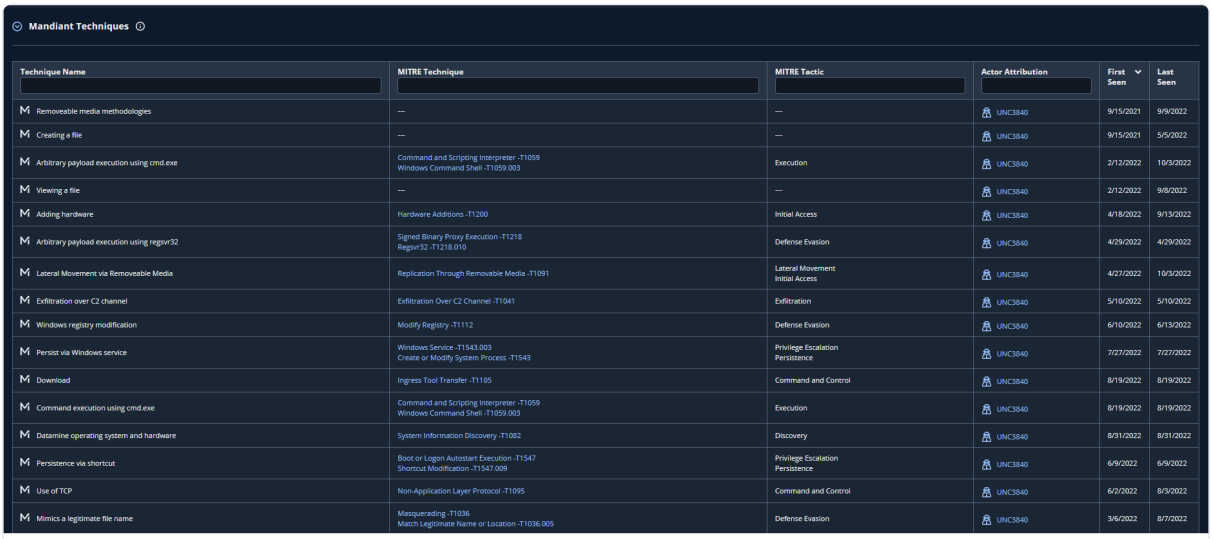
> Click to open the full link in a new tab. This makes it easier to return to your previous view when you're finished reviewing the full details about the campaign.

4. Click **Timeline**. A page appears with two relevant views: **Timeline Overview** (a timeline view of the data in the table below) and **Mandiant Techniques** (more granular details).
5. Optional: Below the Timeline Overview, move the sliders to narrow down or expand the time range, as needed.
6. In the **Timeline Overview** section, click the dots to open a point in time and show the associated Mandiant Technique.



Timeline Overview Highlighting a Mandiant Technique

7. Go to the **Mandiant Techniques** section to see Mandiant Techniques and their mappings to the MITRE ATT@CK framework (techniques and tactics), where applicable. You can also use search terms in any of the headings to filter the table.



Mandiant Techniques Table