EXPLORE MALWARE AND TOOLS

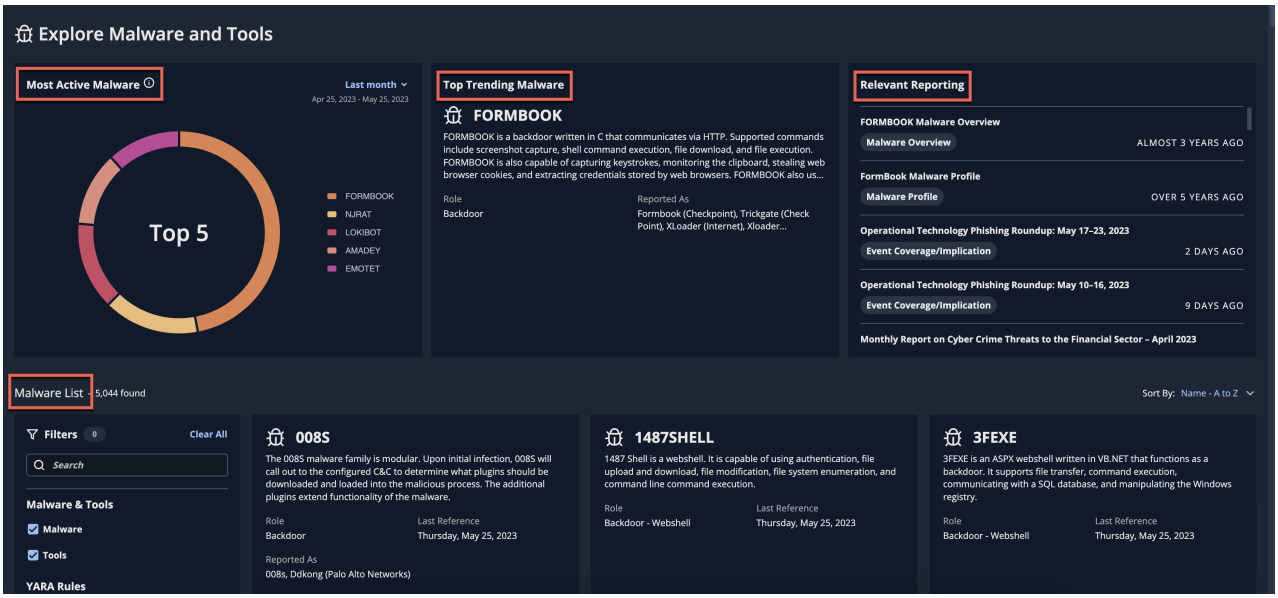
Mandiant Advantage Threat Intelligence (MATI) lets you explore highly contextualized details about Malware families and the Tools used to leverage them.

The Explore Malware and Tools dashboard

To view the **Explore Malware and Tools** dashboard, go to **Explore > Malware and Tools**.

- **Most Active Malware**: Visualization of the five most prolific Malware families that Mandiant is tracking, based on detection rates.
- **Top Trending Malware**: The single most prolific Malware family currently being tracked by Mandiant, including a brief description and other Malware details at a glance.
- **Relevant Reporting**: The most recent finished intelligence reporting from Mandiant related to the most active Malware families.

> Mandiant does not specifically endorse any third-party claims made in this material or related links, and the opinions expressed by third parties are their own.



Filter Malware and Tools

In the **Filters** pane, select the desired filters based on the following options to view only the Malware or Tools you seek to explore.

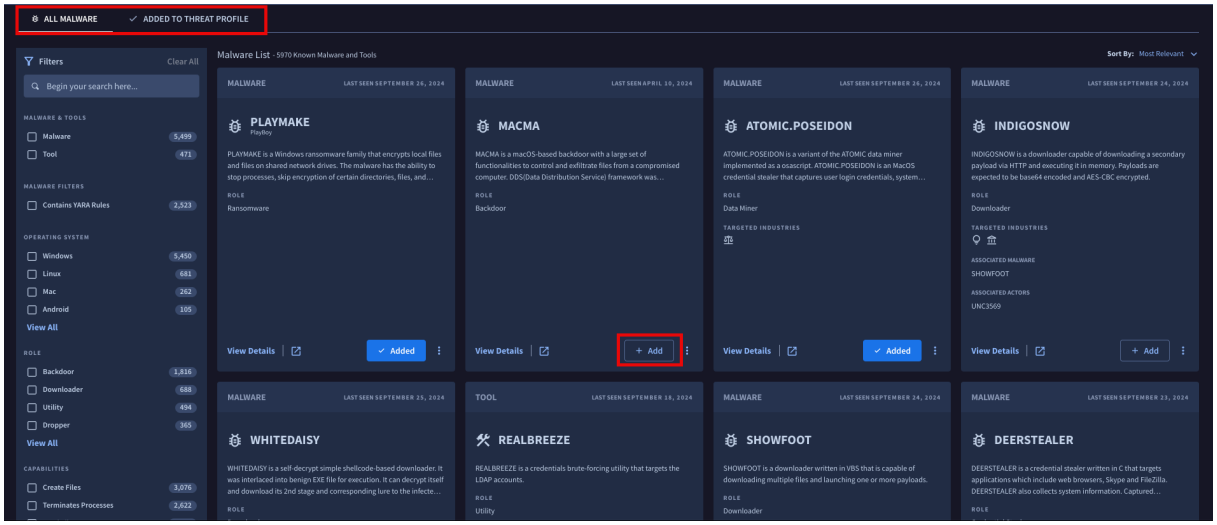
- **Contains YARA Rules**: Display only Malware or Tools that include YARA rules for detection within your environment.
- **Operating System**: Show Malware or Tools that have been observed to target the designated operating systems.
- **Role**: Select the roles of interest that have been observed to be used by the Malware or Tools to be displayed in search results.
- **Capabilities**: Select the capabilities of interest that have been observed to be used by the Malware or Tools to be displayed in search results.

Follow Malware or Tools

In the **All Malware** tab, click **Add** for any Malware or Tool to add it to your Threat Profile. This monitors changes to

selected entities over time, including new variations, associations, or reporting.

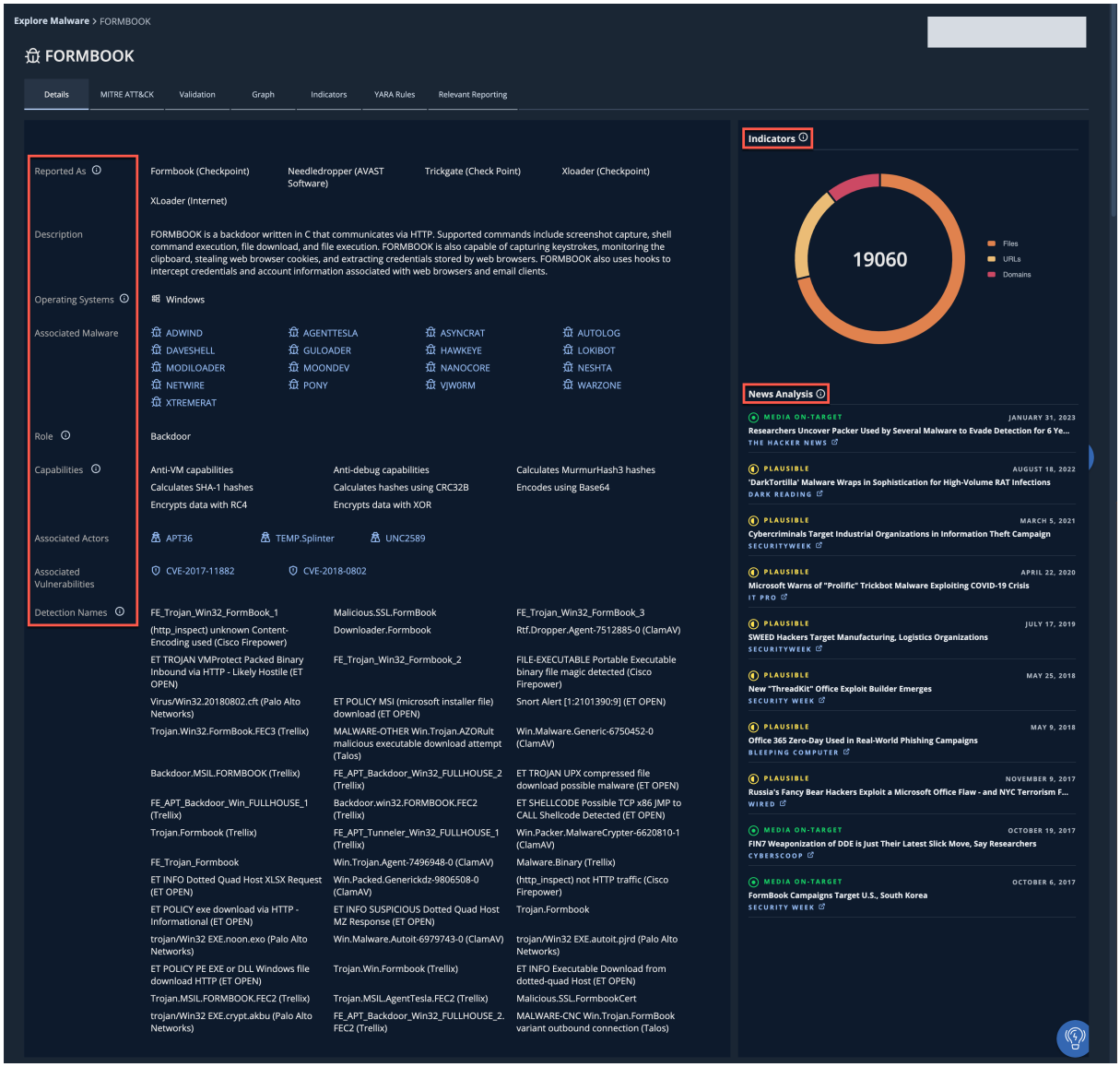
- Navigate to the **Added to Threat Profile** tab to view all the Malware being followed.



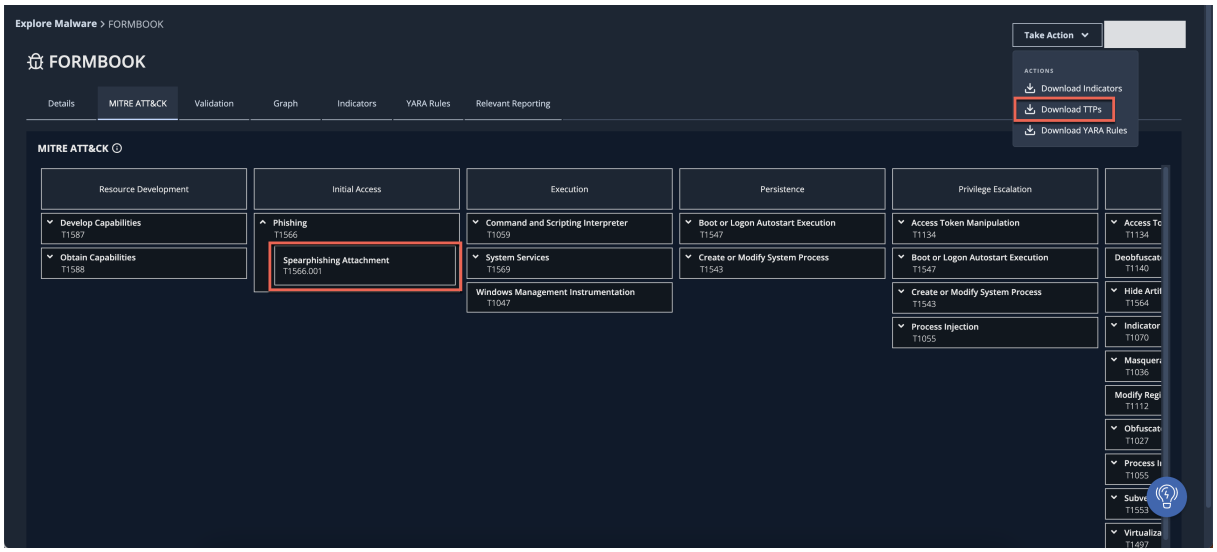
View Malware Details

Select any Malware or Tool for a quick view of a detailed summary. Click **View Full Link** to drill down further into specific components of the Malware profile.

- **Details**: This tab displays the same comprehensive summary of the Malware or tool profile as seen in the quick view. It also includes a visualization of the number of Indicators attributed to the Malware, broken down by type. A list of news analysis reports related to the Malware is also displayed.

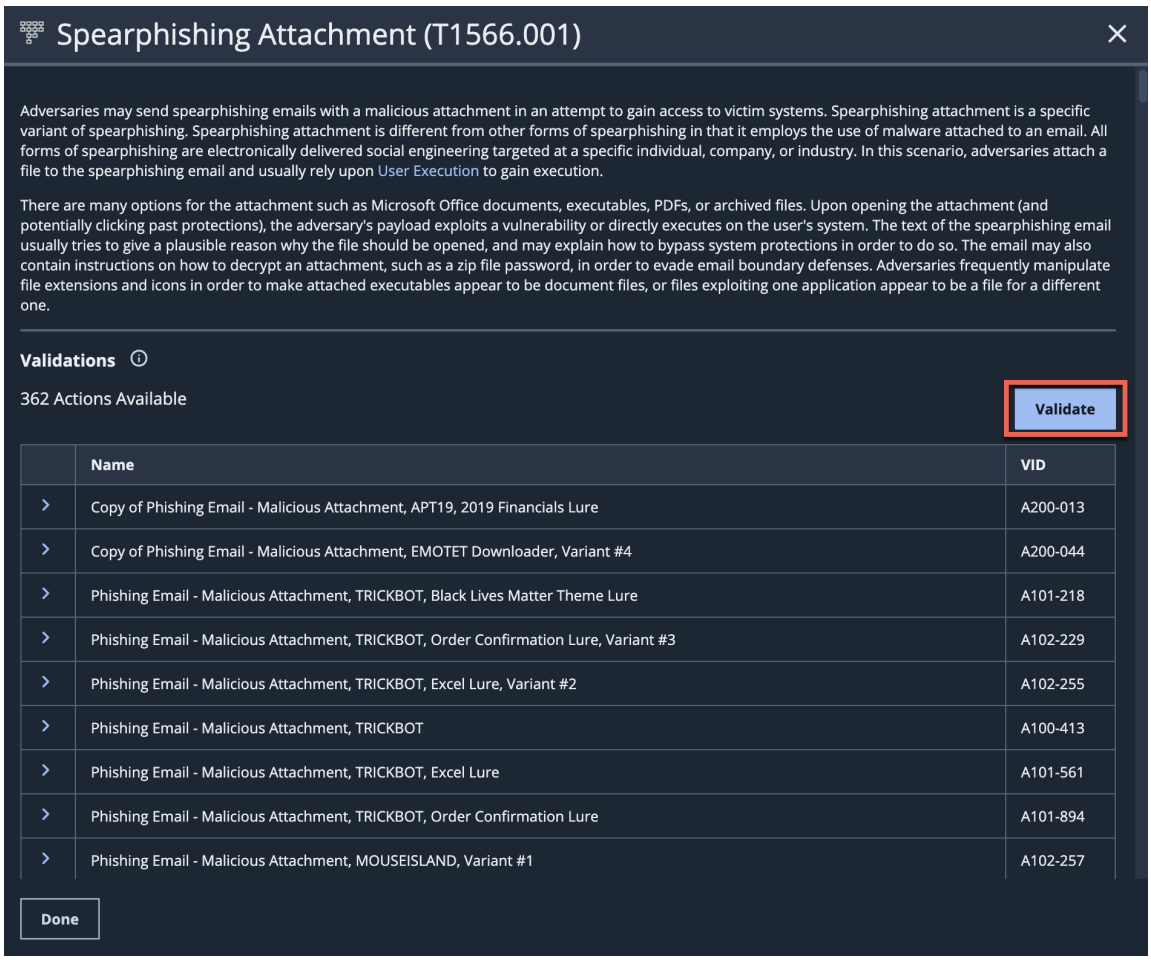


- **MITRE ATT&CK**: This tab shows the Tactics, Techniques, and Procedures (TTPs) observed to be associated with delivering, deploying, or executing the selected Malware. All TTPs associated with the Malware can be downloaded by clicking Download TTPs from the Actions drop-down.



- Selecting a specific technique or subtechnique provides a brief description and a list of Actions that can be used to test your security controls against it. Click **Validate** to pivot directly to the Security Validation platform to execute any of the listed Actions.

> A subscription to Security Validation is required to validate the Actions listed.

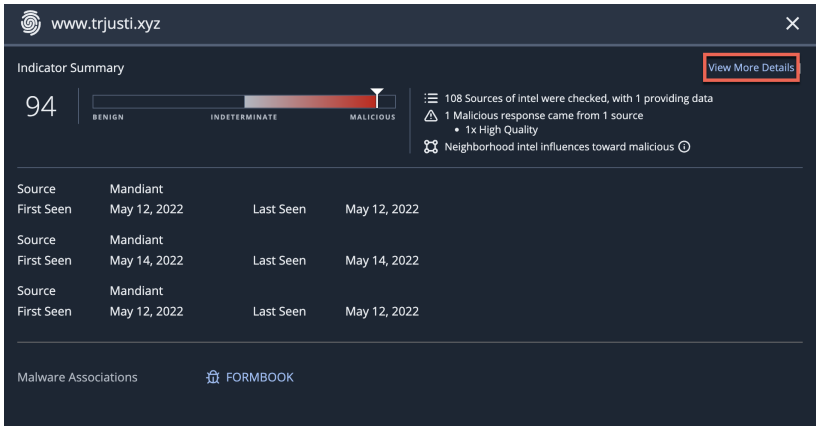


- **Validation**: This tab displays Actions that can be used to test your defenses against this Malware in the Security Validation platform by clicking **Validate**.

  > A subscription to Security Validation is required to validate the Actions listed.

- **Graph**: This tab provides an interactive graph to explore the various associations with this Malware family. The graph includes other associated Malware, attack patterns, Common Vulnerabilities and Exposures (CVEs), indicators of compromise (IOCs), targeted industries, and Threat Actors. Various layout options let you customize your view.

- **Indicators**: This tab includes a table with all known Indicators attributed to this Malware family, such as specific IP addresses, domains, and hashes.
  - **Indicator Value**: Indicators associated with the Malware, with links to pivot directly to the **Indicator Summary**. Click **View Full Link** to view the complete Indicator profile.



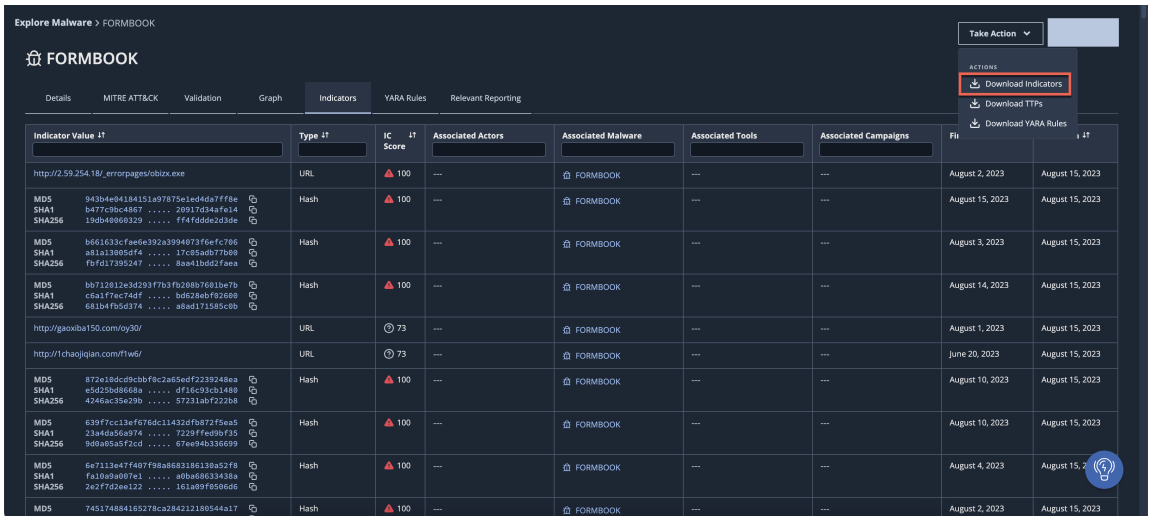
  - **Type**: The type of Indicator (such as IP address, URL, fully qualified domain name (FQDN), or hash).
  - **IC Score**: The probability that a given Indicator is associated with malicious activity (in other words, a true positive).

    > The IC Score is not necessarily a measure of severity or criticality. For more information, see **Understanding IC-Score (https://docs.mandiant.com/home/understanding-ic-score)**.

  - **Associated Actors**: Threat Actors known to be associated with the Indicator, with links to the Threat Actor profile.
  - **Associated Malware**: Other Malware known to be associated with the selected Malware, with links to view

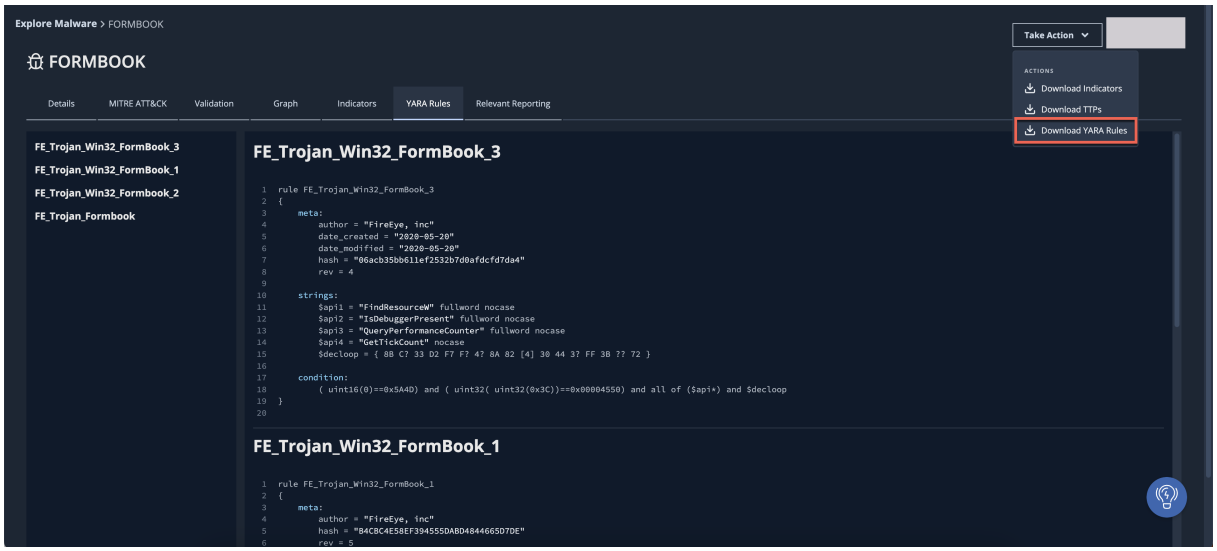
the complete Malware profile.

- **Associated Tools**: Tools observed to be used in association with this Malware.
- **Associated Campaigns**: Threat campaigns associated with the Malware, with links to view the complete Campaign profile.
- **First Seen**: Date when Mandiant last published updates regarding the Malware family.
- **Last Seen**: Date when information on the Malware was first made available to Mandiant customers.
- All Indicators associated with the Threat Actor can be downloaded either by clicking **Download Indicators**.



- **YARA Rules**: This tab displays YARA rules that can be customized to detect this Malware in your environment. These YARA rules can be downloaded for use in threat hunt efforts or other workflows involving third-party security tools outside the MATI platform.

> According to Mandiant's terms of service, any associated detections and subsequent reporting may be distributed as desired.



- **Relevant Reporting**: This tab displays the latest reports generated by Mandiant that are related to or explicitly mention the selected Malware.

The following recording provides a deep dive into getting the most from Mandiant's intelligence related to Malware and

tools: