EXPLORE THREAT ACTORS

Mandiant Advantage Threat Intelligence (MATI) allows you to explore highly contextualized details about Threat Actors, including the ability to follow threat actors' activity over time by adding them to Threat Profiles. You can also easily review relevant reporting and news analysis related to the threat actors. The platform also includes links to quickly pivot to the profiles of correlated threat groups, threat campaigns, targets, malware, tools, and indicators of compromise (IOCs, or simply "indicators") known to be associated with the threat actor.

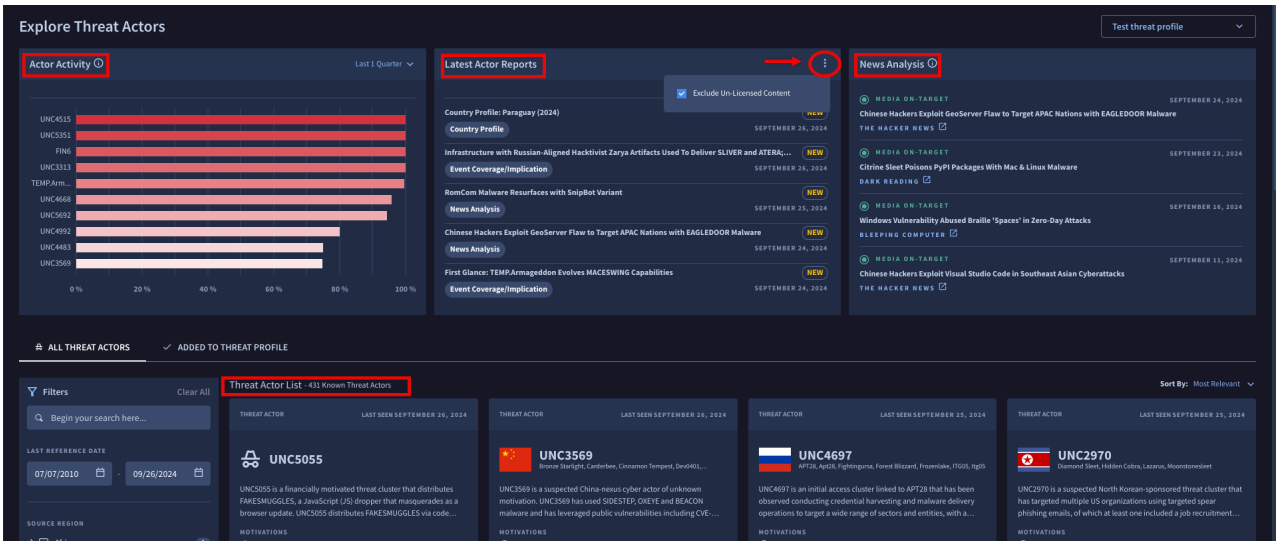
For more information on threat actor tracking and graduation, see **How Does Mandiant Track Threat Actors (https://docs.mandiant.com/home/mati-how-does-mandiant-track-threat-actors).**

To View the Explore Threat Actors dashboard

Go to **Explore > Actors** to view the **Explore Threat Actors** dashboard including the **Threat Actors List** of all Actors being tracked by Mandiant**.**

- **Actor Activity**: Visualization of the volume of changes in threat group activity observed over time, based on an aggregation of data from victim environments, observed actor behavior, and tactics, techniques, and procedures (TTPs) employed.
- **Latest Reports**: Mandiant's most recent finished intelligence reporting spanning all threat actors, report types, regions, and industries. Lists the latest Threat Actor reports generated by Mandiant, with the ability to view only paid subscription reports by checking **Exclude Unlicensed Content**.
- **News Analysis**: Daily expert analysis of current media trends by Mandiant Intelligence to highlight, encapsulate, and provide context to help you frame key, publicly discussed cyber threats.

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.



To Filter Threat Actors

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

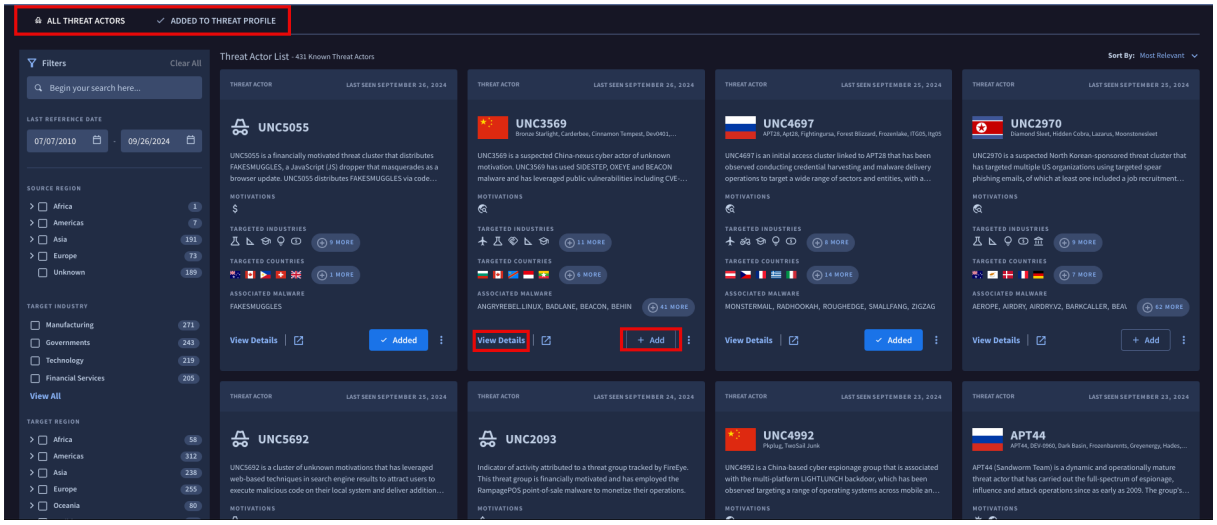
- **Last Seen**: Define the date range in which threat actors of interest are known to have operated.
- **Target Industry**: Select the industries which threat actors of interest are known to target.

- **Target Region**: Select the region(s) in which threat actors of interest are known to operate.
- **Source Region**: Select the region(s) from which threat actors of interest are known to originate.
- **Associated Malware & Tools**: Select the malware and tools known to have been utilized by threat actors of interest.

Add Threat Actors to Threat Profile

In the **All Threat Actors** tab, click **Add** to monitor changes to Threat Actor activity over time, such as their updated use of malware families, tools, and vulnerabilities as part of their TTP.

- Navigate to **Added to Threat Profile** to view all the Threat Actors that you added for Threat Profile tracking.



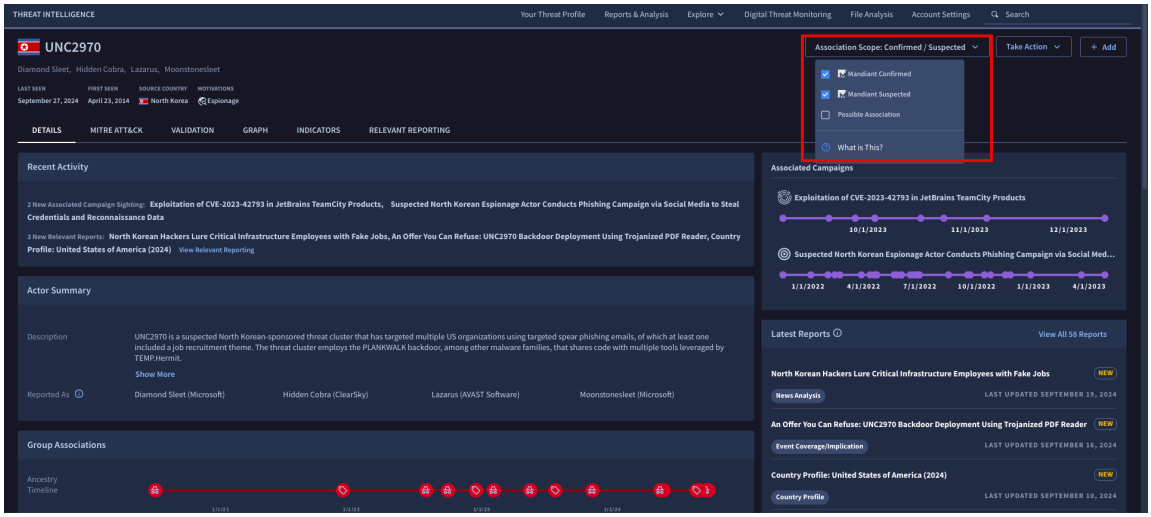
To View Threat Actor Details

Clicking **View Details** for any Threat Actor in the list allows you to drill down into specific components of the Threat Actor's profile.

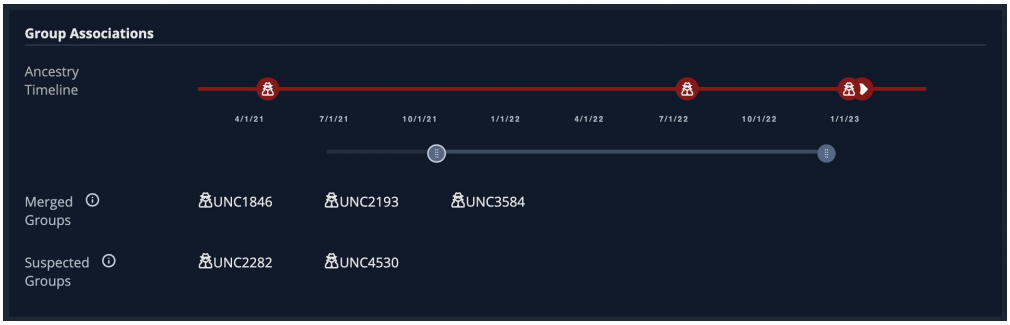
- Click **Association Scope: Confirmed/Suspected** to expand or contract the scope of data displayed based on the assessed confidence in the attribution. For more information, see **Suspected Attribution (https://docs.mandiant.com/home/mati-suspected-attribution)**.
  - **Mandiant Confirmed**: Full confidence attribution
  - **Mandiant Suspected**: Moderate or high confidence attribution
  - **Possible Association**: Low confidence attribution

> This selection is currently reflected on the **Actor Details**, **MITRE ATT&CK**, and **Graph** tabs only and does not apply to the information displayed in the **Indicators** and **Relevant Reporting** tabs.

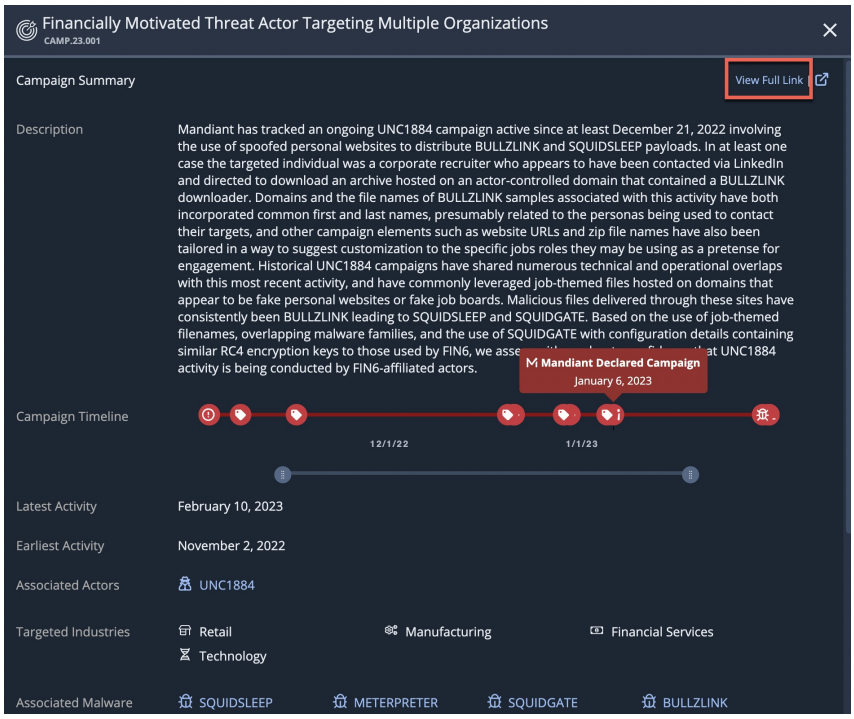
> The default view includes both **Mandiant Confirmed** and **Mandiant Suspected** activity and currently applies to the **Details** and **Graph** tabs only. Items that are only marked **Possible Association** are grayed out in the default view.



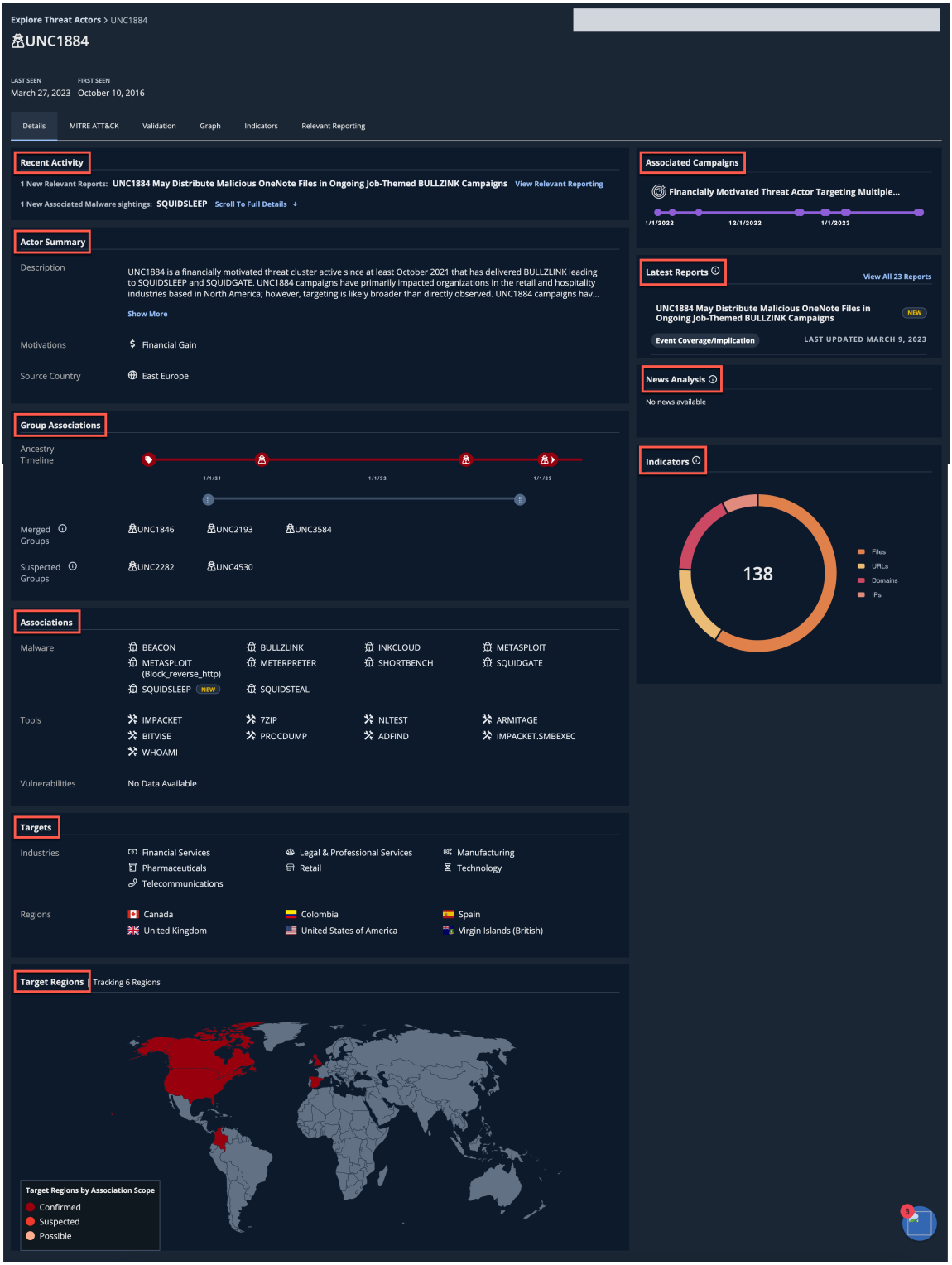
- **Details**: This tab displays a comprehensive summary of the threat actor profile.
  - **Recent Activity**: The latest updates to the threat actor profile by Mandiant.
  - **Actor Summary**: Description of the threat actor including their known **Source Country** and **Motivations** (espionage, financial gain, etc.), if available.
  - **Group Associations**: Threat groups that are either suspected or known to be associated (merged) with the threat actor, including **Ancestry Timeline** with an interactive slider highlighting the evolution of these group associations.
    - **Merged Groups**: Uncategorized (UNC) threat groups that were previously suspected to be related and have since been merged into a named group.
    - **Suspected Groups**: Activity sets that Mandiant believes are related to existing threat groups, but for which there is not enough evidence to attribute the activity with full confidence.



  - **Associations**: Malware, tools, and vulnerabilities that have been attributed to the threat actor.
  - **Targets**: Lists the industries and regions known to be targeted by the threat actor.
  - **Target Regions**: Visualization of regions targeted by the threat actor, broken down by **Association Scope**.
  - **Associated Campaigns**: Threat campaigns associated with the threat actor, with links to pivot directly into the **Campaign Summary** including an interactive **Campaign Timeline**. Click **View Full Link** to explore the complete campaign profile.

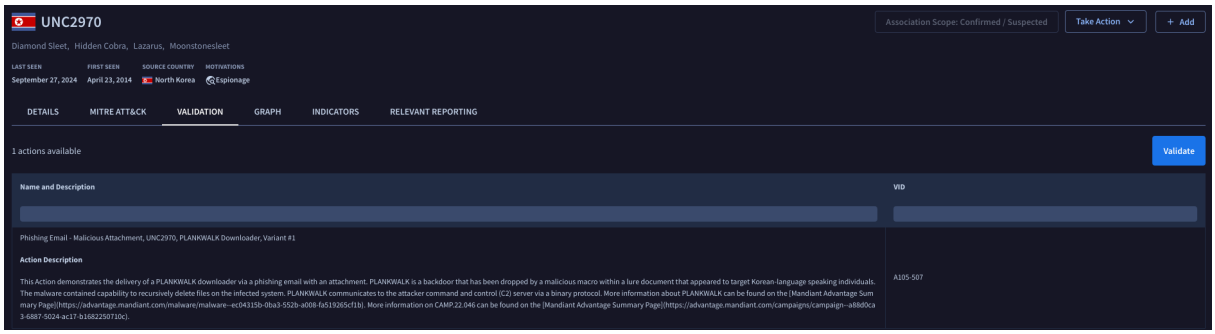


- **Latest Reports**: Mandiant's most recent finished intelligence reporting for this Threat Actor, spanning all report types, regions, and industries.
- **News Analysis**: Expert analysis of current media trends by Mandiant Intelligence to highlight, encapsulate, and provide context to help you frame key, publicly discussed cyber threats related to this actor.
- **Indicators**: Number of released indicators attributed to the threat actor, broken down by indicator type.

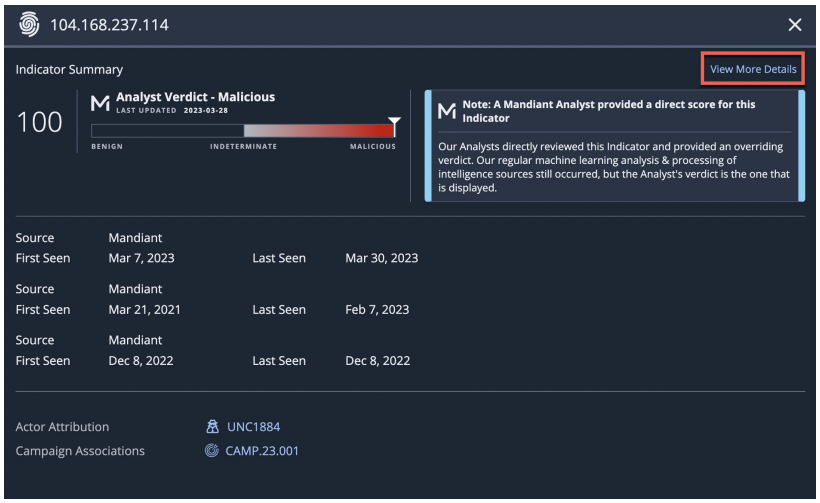


- **MITRE ATT&CK**: This tab shows the Tactics, Techniques, and Procedures (TTPs) observed to be used by this threat actor.
- **Validation**: This tab displays Actions that can be used to test your defenses against this Threat Actor in the Validation Platform, if available.

> Using Actions to validate your security controls requires a subscription to Security Validation.



- **Graph**: This tab provides an interactive graph to explore the various associations with this Threat Actor including industries, malware, attack patterns, and indicators.
- **Indicators**: This tab includes a table with all known indicators attributed to this Threat Actor, such as specific IP addresses, domains, and hashes.
    - **Indicator Value**: Indicators associated with the threat actor, with links to pivot directly to the **Indicator Summary**. Click **View Full Link** to view the complete indicator profile.



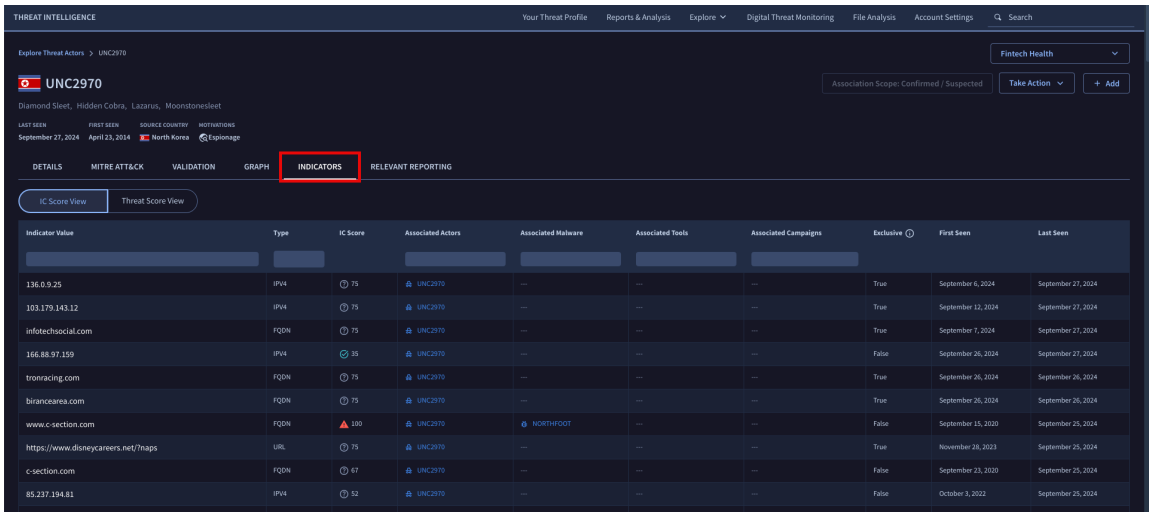
    - **Type**: The type of indicator (IP address, URL, fully qualified domain name (FQDN), hash, etc.).
    - **IC Score**: The probability that a given indicator is associated with malicious activity (in other words, a true positive).

> 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 actor(s) known to be associated with the indicator, with links to the threat actor profile(s).
    - **Associated Malware**: Malware known to be associated with the indicator, with links to pivot directly into the **Malware Summary**. Click **View Full Link** to view the complete malware profile.
    - **Associated Campaigns**: Threat campaigns associated with the threat actor, with links to pivot directly into the **Campaign Summary**. Click **View Full Link** to view the complete campaign profile.
    - **Exclusive**: An indicator that Mandiant can explicitly attribute to a single threat actor.

> Indicators that have the possibility of being leveraged by multiple threat actors, such as an IP address, are not considered exclusive.

- **First Seen**: Date when information on the threat actor was first made available to Mandiant customers.
- **Last Seen**: Date when Mandiant last published updates regarding the threat actor.



- **Relevant Reporting**: This tab lists all reports in which this Threat Actor was mentioned, further broken down by Report Type and Published Date.
- All indicators associated with the Threat Actor can be downloaded either by clicking **Download Indicators** or the More menu ⋮ on the Threat Actor entry in the Threat Actors list.

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

Threat Actors Overview

The following video provides a quick overview of navigating the Threat Actors web interface:

Threat Actors Deep Dive

The following recording from one of our Principal Architects provides a deep dive into getting the most from Mandiant's Threat Actor intelligence: