

SEARCH THREAT INTELLIGENCE CONTENT IN MATI

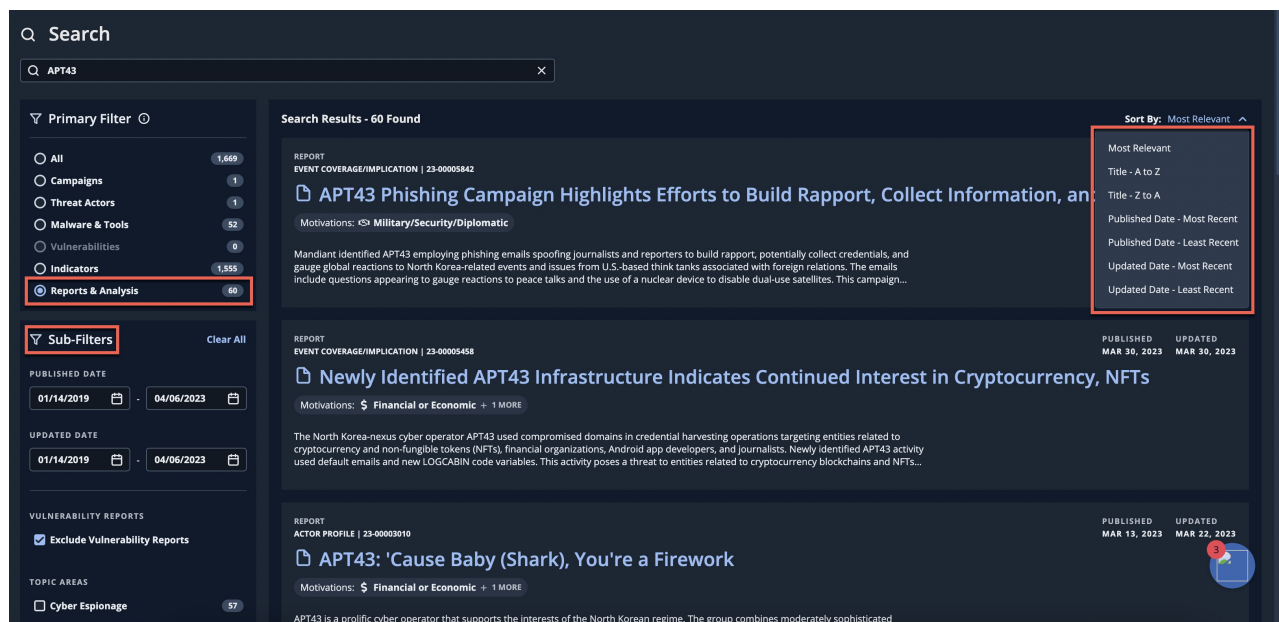
Mandiant Advantage Threat Intelligence (MATI) provides Advanced Search capabilities to help you easily navigate Mandiant's vast knowledge base of threat intelligence data to drill down to what's relevant and quickly pivot to explore associated campaigns, threat actors, vulnerabilities, indicators, malware, tools, and reports & analysis.



Initial search results will be sorted by **Most Relevant**; no other sorting options are available until a **Primary Filter** is applied.

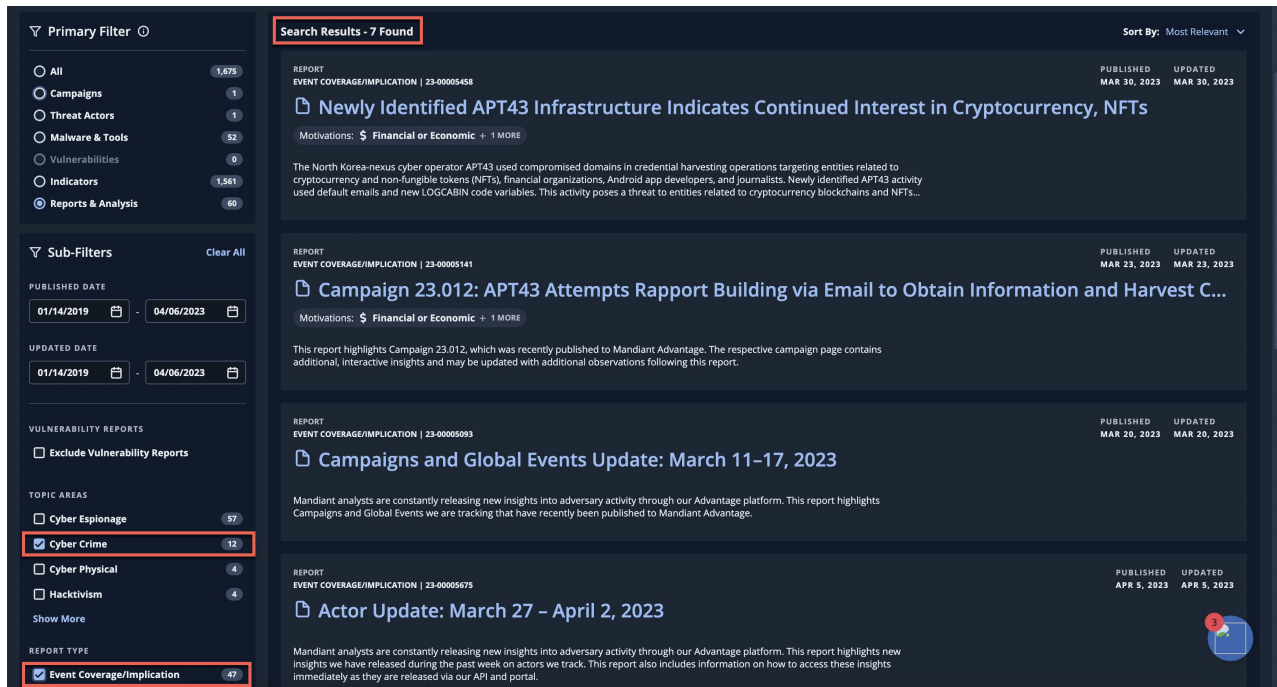
Filtering

Once a **Primary Filter** has been selected, additional **Sub-Filters** and **Sort By** options that are specific to the **Primary Filter** will become available.



The screenshot displays the Mandiant MATI search interface. On the left, the 'Search' sidebar is visible with a search bar containing 'APT43'. Below the search bar, the 'Primary Filter' section shows 'Reports & Analysis' selected, with a count of 60. The 'Sub-Filters' section includes 'Published Date' (01/14/2019 to 04/06/2023), 'Updated Date' (01/14/2019 to 04/06/2023), 'Vulnerability Reports' (Exclude Vulnerability Reports checked), and 'Topic Areas' (Cyber Espionage selected, 97). The main search results area shows 60 results. The top result is a report titled 'APT43 Phishing Campaign Highlights Efforts to Build Rapport, Collect Information, and...' with a 'Sort By' dropdown menu open, showing options: 'Most Relevant', 'Title - A to Z', 'Title - Z to A', 'Published Date - Most Recent', 'Published Date - Least Recent', 'Updated Date - Most Recent', and 'Updated Date - Least Recent'. The second result is 'Newly Identified APT43 Infrastructure Indicates Continued Interest in Cryptocurrency, NFTs'. The third result is 'APT43: 'Cause Baby (Shark), You're a Firework'.

Once you select a primary filter for the search criteria, each sub-filter will display the number of associated matches for that search criteria. If sub-filters are selected from different sub-filter categories, the AND operator is used to combine the total search results.



Primary Filter ○

- All 1,675
- Campaigns 1
- Threat Actors 1
- Malware & Tools 52
- Vulnerabilities 0
- Indicators 1,561
- Reports & Analysis 60

Sub-Filters Clear All

PUBLISHED DATE: 01/14/2019 - 04/06/2023

UPDATED DATE: 01/14/2019 - 04/06/2023

VULNERABILITY REPORTS

Exclude Vulnerability Reports

TOPIC AREAS

- Cyber Espionage 57
- Cyber Crime 12
- Cyber Physical 4
- Hacktivism 4

Show More

REPORT TYPE

- Event Coverage/Implication 47

Search Results - 7 Found

Sort By: Most Relevant ▼

REPORT
EVENT COVERAGE/IMPLICATION | 23-00005458
PUBLISHED: MAR 30, 2023
UPDATED: MAR 30, 2023

Newly Identified APT43 Infrastructure Indicates Continued Interest in Cryptocurrency, NFTs

Motivations: 🇺🇸 Financial or Economic + 1 MORE

The North Korea-nexus cyber operator APT43 used compromised domains in credential harvesting operations targeting entities related to cryptocurrency and non-fungible tokens (NFTs), financial organizations, Android app developers, and journalists. Newly identified APT43 activity used default emails and new LOGCABIN code variables. This activity poses a threat to entities related to cryptocurrency blockchains and NFTs...

REPORT
EVENT COVERAGE/IMPLICATION | 23-00005141
PUBLISHED: MAR 23, 2023
UPDATED: MAR 23, 2023

Campaign 23.012: APT43 Attempts Rapport Building via Email to Obtain Information and Harvest C...

Motivations: 🇺🇸 Financial or Economic + 1 MORE

This report highlights Campaign 23.012, which was recently published to Mandiant Advantage. The respective campaign page contains additional, interactive insights and may be updated with additional observations following this report.

REPORT
EVENT COVERAGE/IMPLICATION | 23-00005093
PUBLISHED: MAR 20, 2023
UPDATED: MAR 20, 2023

Campaigns and Global Events Update: March 11-17, 2023

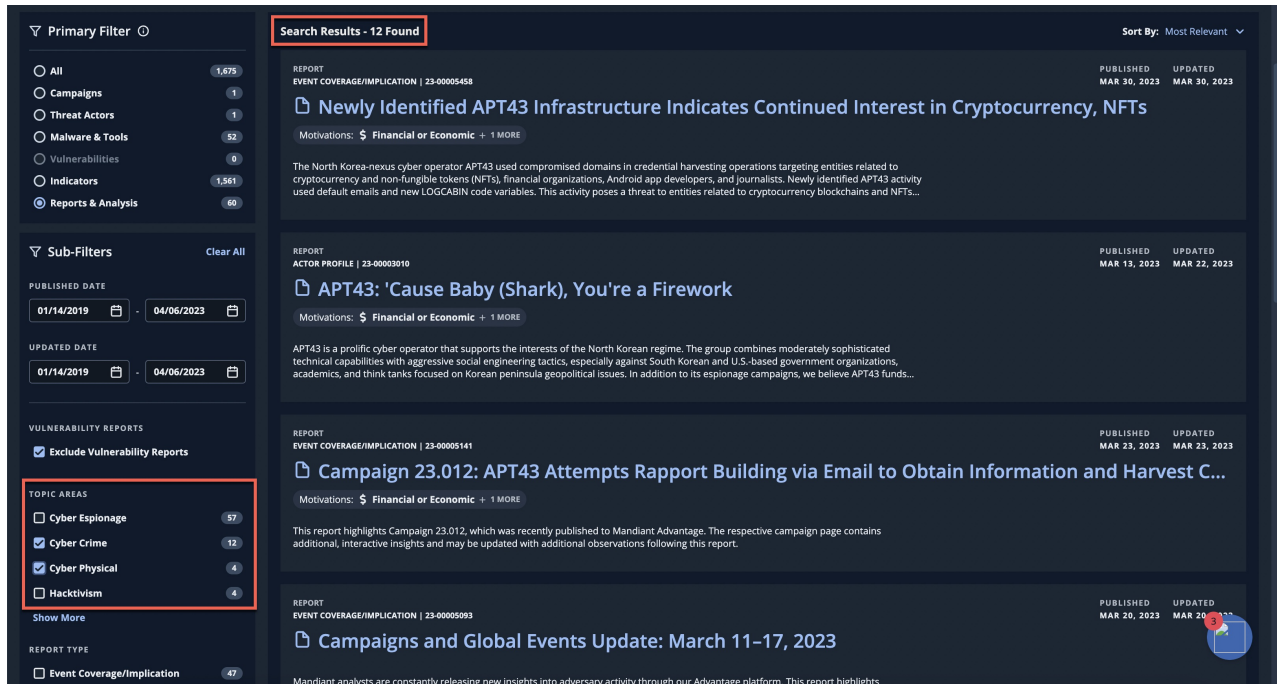
Mandiant analysts are constantly releasing new insights into adversary activity through our Advantage platform. This report highlights Campaigns and Global Events we are tracking that have recently been published to Mandiant Advantage.

REPORT
EVENT COVERAGE/IMPLICATION | 23-00005675
PUBLISHED: APR 5, 2023
UPDATED: APR 5, 2023

Actor Update: March 27 - April 2, 2023

Mandiant analysts are constantly releasing new insights into adversary activity through our Advantage platform. This report highlights new insights we have released during the past week on actors we track. This report also includes information on how to access these insights immediately as they are released via our API and portal.

If multiple sub-filters are selected within the same sub-filter category, the OR operator is used to combine the total search results.



Primary Filter ○

- All 1,675
- Campaigns 1
- Threat Actors 1
- Malware & Tools 52
- Vulnerabilities 0
- Indicators 1,561
- Reports & Analysis 60

Sub-Filters Clear All

PUBLISHED DATE: 01/14/2019 - 04/06/2023

UPDATED DATE: 01/14/2019 - 04/06/2023

VULNERABILITY REPORTS

Exclude Vulnerability Reports

TOPIC AREAS

- Cyber Espionage 57
- Cyber Crime 12
- Cyber Physical 4
- Hacktivism 4

Show More

REPORT TYPE

- Event Coverage/Implication 47

Search Results - 12 Found

Sort By: Most Relevant ▼

REPORT
EVENT COVERAGE/IMPLICATION | 23-00005458
PUBLISHED: MAR 30, 2023
UPDATED: MAR 30, 2023

Newly Identified APT43 Infrastructure Indicates Continued Interest in Cryptocurrency, NFTs

Motivations: 🇺🇸 Financial or Economic + 1 MORE

The North Korea-nexus cyber operator APT43 used compromised domains in credential harvesting operations targeting entities related to cryptocurrency and non-fungible tokens (NFTs), financial organizations, Android app developers, and journalists. Newly identified APT43 activity used default emails and new LOGCABIN code variables. This activity poses a threat to entities related to cryptocurrency blockchains and NFTs...

REPORT
ACTOR PROFILE | 23-00003910
PUBLISHED: MAR 13, 2023
UPDATED: MAR 22, 2023

APT43: 'Cause Baby (Shark), You're a Firework

Motivations: 🇺🇸 Financial or Economic + 1 MORE

APT43 is a prolific cyber operator that supports the interests of the North Korean regime. The group combines moderately sophisticated technical capabilities with aggressive social engineering tactics, especially against South Korean and U.S.-based government organizations, academics, and think tanks focused on Korean peninsula geopolitical issues. In addition to its espionage campaigns, we believe APT43 funds...

REPORT
EVENT COVERAGE/IMPLICATION | 23-00005141
PUBLISHED: MAR 23, 2023
UPDATED: MAR 23, 2023

Campaign 23.012: APT43 Attempts Rapport Building via Email to Obtain Information and Harvest C...

Motivations: 🇺🇸 Financial or Economic + 1 MORE

This report highlights Campaign 23.012, which was recently published to Mandiant Advantage. The respective campaign page contains additional, interactive insights and may be updated with additional observations following this report.

REPORT
EVENT COVERAGE/IMPLICATION | 23-00005093
PUBLISHED: MAR 20, 2023
UPDATED: MAR 20, 2023

Campaigns and Global Events Update: March 11-17, 2023

Mandiant analysts are constantly releasing new insights into adversary activity through our Advantage platform. This report highlights



Keep in mind that search criteria may appear in multiple sub-filters, even within the same sub-filter category. As different combinations of sub-filters are selected (using AND across categories, and OR within categories), the match count at the top of the list of search results will update accordingly.

Video overview

The following video provides a quick walk through of Advanced Search capabilities:

Gemini search notice

After Nov 7, 2024, the Gemini search functionality in Mandiant Advantage is no longer available. We are excited to offer you a more powerful and comprehensive platform for investigating and responding to threats through Google Threat Intelligence (Google TI). We have incorporated your feedback from the Gemini search in MATI into the Google TI version of the product.

Google TI offers a more comprehensive and powerful search experience, leveraging the latest Gemini models and incorporating a broader range of data sources.

What to expect



- **More Comprehensive Data:** Google TI combines threat intelligence from Mandiant, Google, and VirusTotal, providing a more complete view of the threat landscape. This includes signals from VirusTotal's massive threat database and Google's own telemetry, giving you a richer understanding of potential threats.
- **Faster and More Informative Answers:** The search functionality in Google TI utilizes the latest Gemini models, enabling faster and more relevant search results. You'll be able to find the information you need more quickly and efficiently.
- **Enhanced Features:** Google TI offers an improved search experience with new features, including the ability to search across OSINT articles. This provides you with even greater insights and context when investigating threats.

Need help?

Visit [our website](#) or [contact our team](#) to learn more and get started with Google TI. Our team is available to assist you and answer any questions you may have.