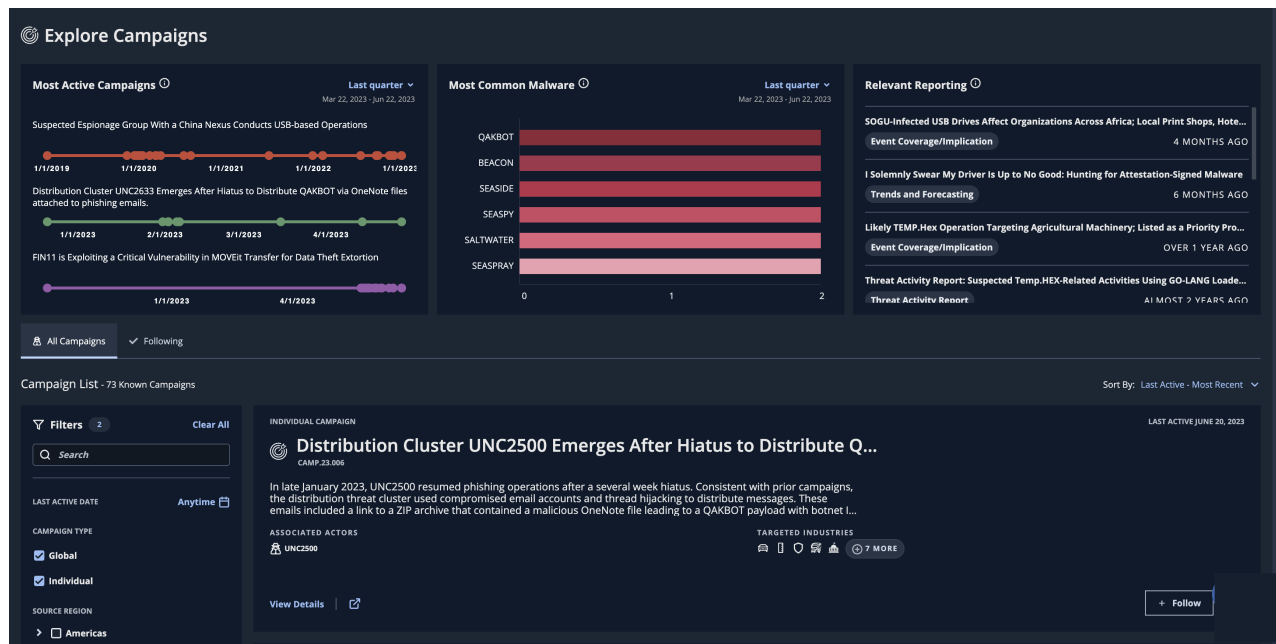


THREAT CAMPAIGNS

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

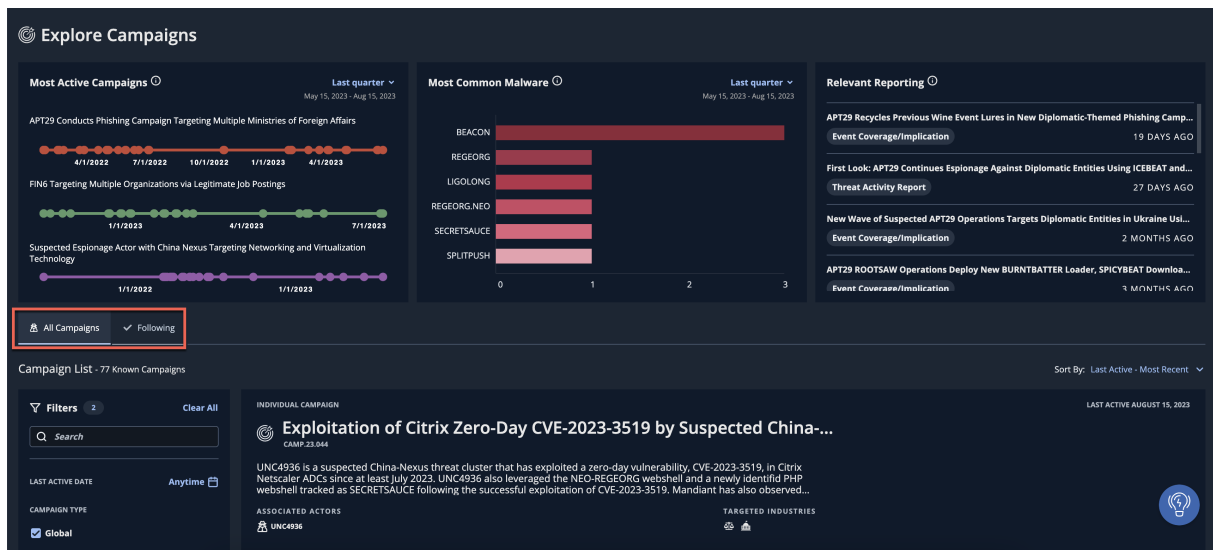
Campaigns provide the following features:

- **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.

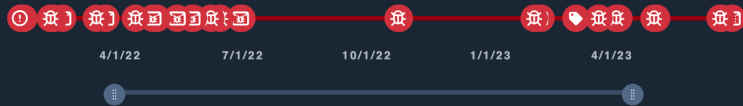

APT29 Conducts Phishing Campaign Targeting Multiple Ministries of Foreign Affairs
CAMP.22.005
✕

Campaign Summary
[View Full Link](#) | 

Description

Since at least January 17, 2022, APT29 has carried out a phishing campaign using compromised email accounts to primarily target European diplomatic entities and distribute a new downloader dubbed BEATDROP as well as a downloader BOOMMIC after establishing access. Beginning in October 2022, APT29 began leveraging a new variant of the BEATDROP downloader, tracked as FANCYBEAT, in phishing campaigns against similar targets. Continued tensions and the threat of Russian invasion into Ukraine corresponds with increased cyber activity from Russian-nexus operators such as APT29, especially against targets in Eastern Europe and in government and diplomatic organizations. APT29 is a cyber espionage operation which has leveraged innovative tactics, techniques, and procedures against humanitarian groups, think tanks, defense, and diplomatic institutions in Europe and North America since at least March 2021.


Campaign Timeline



Latest Activity June 30, 2023

Earliest Activity January 17, 2022

Reported Associations


 Cloaked Ursa (Palo Alto Networks)


 Envyscout (Palo Alto Networks)

Associated Actors









 APT29

Targeted Industries





 Governments

 Telecommunications

Associated Malware

 LOUDGUEST	 BEACON	 BEATDROP (Slack)	 STATICNOISE
 DONUT	 SALTSHAKER	 BEATDROP (Dropbox)	 BEATDROP
 BOOMMIC	 MUSKYBEAT	 ROOTSAW	 DAVESHELL
 ICEBREAKER	 BEATDROP.NOTION	 BURNTBATTER	 BEATDROP (Trello)
 LINKSHELL	 SPICYBEAT		










Associated Tools

 COBALTSTRIKE	 RUBEUS	 ADFIND	 NLTEST
 WHOAMI			

Source Regions

 Russia

Targeted Regions

 Ukraine	 India	 Poland	 Italy
 Czech Republic	 Portugal	 Austria	 Belgium
 Denmark	 Greece	 Montenegro	 Turkey
 Switzerland	 Spain	 Canada	


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.



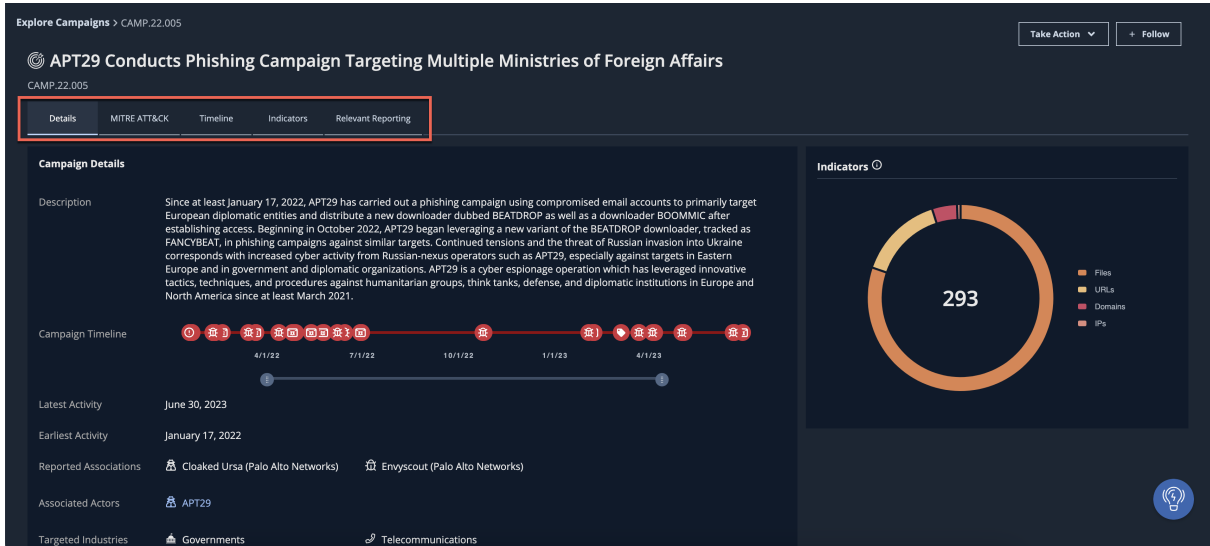
Some campaigns are part of a larger (global) campaign. These campaigns also include associated campaigns in the details view. You can click those campaign links and go to the detail view for the individual campaigns. The associations that may also appear are related actors, related malware families,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

- 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.



Explore Campaigns > CAMP.22.005

Take Action + Follow

APT29 Conducts Phishing Campaign Targeting Multiple Ministries of Foreign Affairs

CAMP.22.005

Details MITRE ATT&CK Timeline Indicators Relevant Reporting

Campaign Details

Description: Since at least January 17, 2022, APT29 has carried out a phishing campaign using compromised email accounts to primarily target European diplomatic entities and distribute a new downloader dubbed BEATDROP as well as a downloader BOOMMIC after establishing access. Beginning in October 2022, APT29 began leveraging a new variant of the BEATDROP downloader, tracked as FANCYBEAT, in phishing campaigns against similar targets. Continued tensions and the threat of Russian invasion into Ukraine corresponds with increased cyber activity from Russian-nexus operators such as APT29, especially against targets in Eastern Europe and in government and diplomatic organizations. APT29 is a cyber espionage operation which has leveraged innovative tactics, techniques, and procedures against humanitarian groups, think tanks, defense, and diplomatic institutions in Europe and North America since at least March 2021.

Campaign Timeline: 4/1/22 7/1/22 10/1/22 1/1/23 4/1/23

Latest Activity: June 30, 2023

Earliest Activity: January 17, 2022

Reported Associations: Cloaked Ursa (Palo Alto Networks), Enviscout (Palo Alto Networks)

Associated Actors: APT29

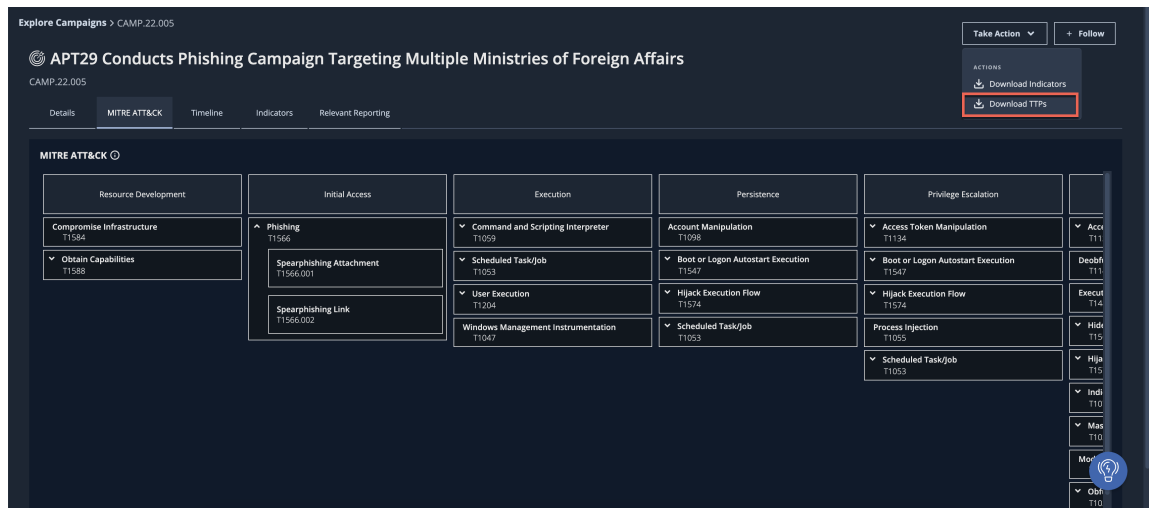
Targeted Industries: Governments, Telecommunications

Indicators

293

- Files
- URLs
- Domains
- IPs

- 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** dropdown.



Explore Campaigns > CAMP.22.005

Take Action + Follow

APT29 Conducts Phishing Campaign Targeting Multiple Ministries of Foreign Affairs

CAMP.22.005

Details MITRE ATT&CK Timeline Indicators Relevant Reporting

MITRE ATT&CK

Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Account Manipulation
<ul style="list-style-type: none"> Compromise Infrastructure T1584 Obtain Capabilities T1588 	<ul style="list-style-type: none"> Phishing T1566 <ul style="list-style-type: none"> Spearphishing Attachment T1566.001 Spearphishing Link T1566.002 	<ul style="list-style-type: none"> Command and Scripting Interpreter T1059 <ul style="list-style-type: none"> Scheduled Task/Job T1053 User Execution T1204 Windows Management Instrumentation T1047 	<ul style="list-style-type: none"> Account Manipulation T1098 <ul style="list-style-type: none"> Boot or Logon Autostart Execution T1547 Hijack Execution Flow T1574 Scheduled Task/Job T1053 	<ul style="list-style-type: none"> Access Token Manipulation T1134 <ul style="list-style-type: none"> Boot or Logon Autostart Execution T1547 Hijack Execution Flow T1574 Process Injection T1055 Scheduled Task/Job T1053 	<ul style="list-style-type: none"> Account Manipulation T111 Deobf T11 Execut T14 Hide T15 Hija T15 Indi T10 Max T10 Mea T10 Oba T10

ACTIONS

- Download Indicators
- Download TTPs

- Click **Timeline** to access the following:
 - A more detailed view of the timeline for the campaign. For more details, see [Mandiant Techniques \(https://docs.mandiant.com/home/mandiant-techniques\)](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 \(https://docs.mandiant.com/home/mandiant-techniques\)](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.

Explore Campaigns > CAMP.22.005

APT29 Conducts Phishing Campaign Targeting Multiple Ministries of Foreign Affairs
CAMP.22.005

Details MITRE ATT&CK Timeline Indicators Relevant Reporting

Take Action + Follow

ACTIONS
Download Indicators
Download TTPs

Indicator Value ¹	Type ¹	IC Score ¹	Associated Actors	Associated Malware	Associated Tools	Associated Campaigns	Exclusive ¹	First Seen ¹	Last Seen ¹
MDS e3063330939ea198f44416d25449784a SHA1 fd45d69af80f 523aad22bbd15 SHA256 79a1402bc77a ca668ce0d1b1f8	Hash	100	APT29	BURNBATTER	---	CAMP.22.005	True	May 4, 2023	August 4, 2023
MDS 854e5c92e93b698ab8d8c8a8b673f SHA1 8128e1f04130 8a47956336645d SHA256 8dd95a2349e8 39f47abe59429	Hash	74	APT29	---	---	CAMP.22.005	True	March 28, 2023	August 4, 2023
MDS 8033b9ebdc41e01923fbc25f8a8a80 SHA1 ec4017798790 88564e8e4234 SHA256 c62199ef9c27 5deaa663158a7	Hash	100	APT29	DONUT	---	CAMP.22.005	True	May 4, 2023	August 4, 2023
MDS 1290a1e7c813fd8c2843d9ec191e39e SHA1 29bab281b479 b7c8ae39ca62d SHA256 68d9e6d03409 3c841945d58e	Hash	100	APT29	BURNBATTER	---	CAMP.22.005	True	March 28, 2023	July 31, 2023
MDS 1b371d33e9b5acfa78a478d289b62388 SHA1 a8805f788220 f4e8c2a34721b SHA256 94633305a575 38ea34ca95f1	Hash	100	APT29	MUSKYBEAT	---	CAMP.22.005	True	April 12, 2023	July 29, 2023
MDS 9a3308b498ed08e177f1782e8d90a07 SHA1 fa71067f418 5533e66fd99e2 SHA256 7fc9e830756e f4caeb2a83cd	Hash	100	APT29	STATICNOISE	---	CAMP.22.005	True	June 22, 2023	July 28, 2023
MDS e8779de6644430ec9b1d62e437807c SHA1 7737e9b8ecec a98ffccc65e8ff SHA256 3da1f49e7f19 806c346584112	Hash	100	APT29	ROOTSAW	---	CAMP.22.005	True	June 23, 2023	July 28, 2023
www.sembomstilauseutie.no	FQDN	44	APT29	---	---	CAMP.22.005	False	June 23, 2023	July 28, 2023

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