

Attack Flow Training: 4 – Building An Attack Flow

May 14, 2025 • Brussels



Agenda

- 1 – Introduction to Attack Flow
- 2 – Tagging Techniques in Narrative Reports

Break

- 3 – Using Attack Flow Builder
- *Lightning Talk*
- 4 – Building An Attack Flow

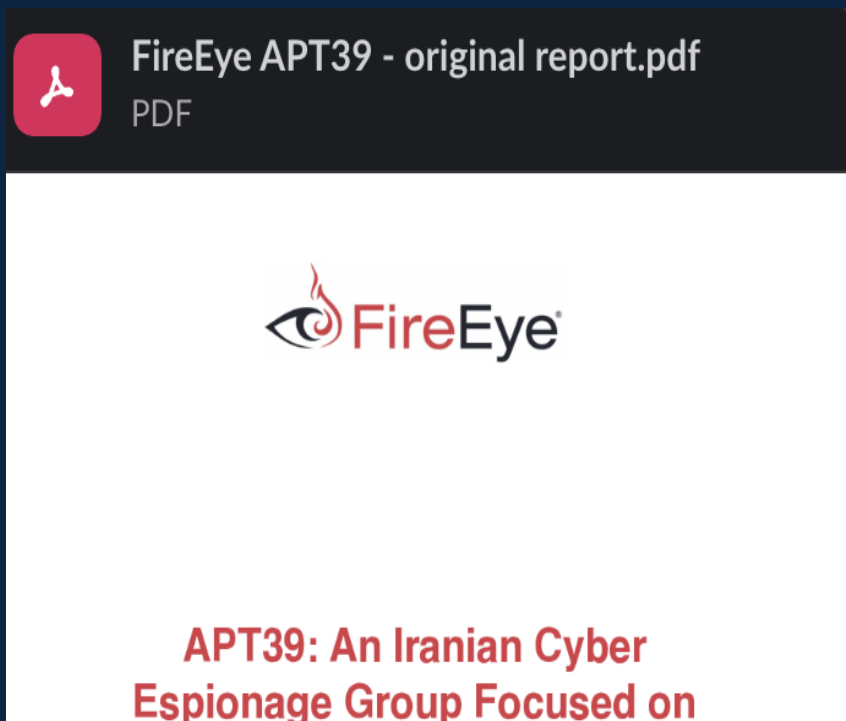
Break

- *Lightning Talk*
- 5 – Attack Flow 3 Preview
- *Lightning Talk*
- 6 – Visualization

Building Attack Flows from CTI Reports

- Attack Flow helps CTI teams transform threat data into structured, sequential, visual narratives that improve analysis, reporting, and decision-making.
- Seamlessly combine IOCs (Indicators of Compromise) with IOBs (Indicators of Behavior).
- Identify and reduce ambiguity that is present in prose.
- The process of building a flow can point in the direction for future investigation: what questions remain? What ambiguities to resolve?

Step 1: Read the Report and Annotate techniques



Attack Lifecycle

APT39 uses a variety of custom tools throughout the attack lifecycle.

1. Initial Access - Phishing: Spearphishing Attachment (T1566.001)
2. Initial Access - Phishing: Spearphishing Link (T1566.002)
3. Execution - User Execution: Malicious File (T1204.002)
4. Execution - User Execution: Malicious Link (T1204.001)

Initial Compromise

For initial compromise, FireEye Intelligence has observed APT39 leverage spear phishing emails with malicious attachments and/or hyperlinks typically resulting in a POWBAT infection. APT39 frequently registers and leverages domains that masquerade as legitimate web services and organizations that are relevant to the intended target.

Furthermore, this group has routinely identified and exploited vulnerable web servers of targeted organizations to install web shells, such as ANTAK and ASPXSPY, and used stolen legitimate credentials to compromise externally facing Outlook Web Access (OWA)

6. Initial Access - Valid Accounts (T1078)

7. Credential Access - C

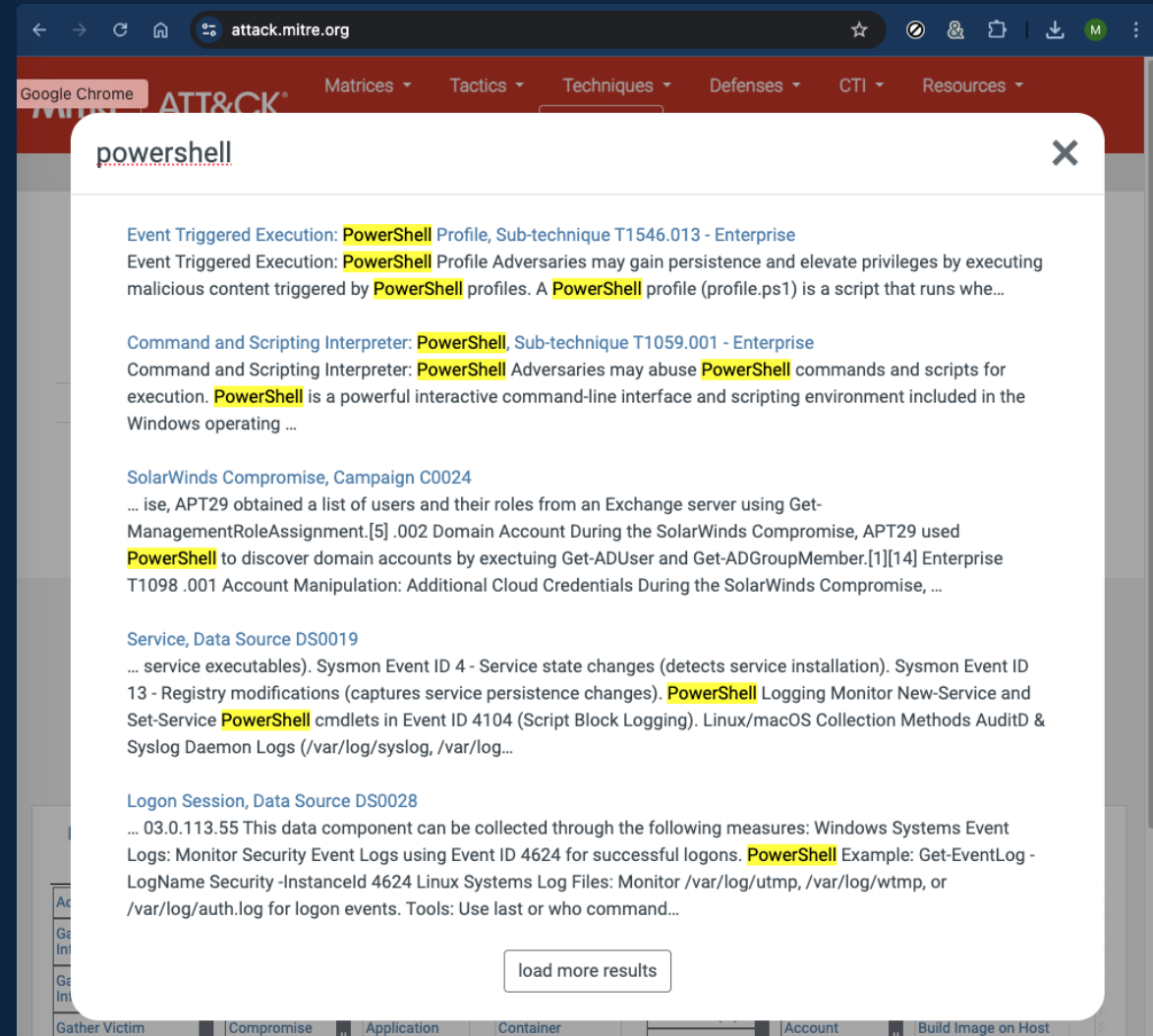
Establish Foothold, Escalate Privileges, and Internal Reconnaissance

5. Persistence

Post-compromise, APT39 leverages custom backdoors such as SEAWEED, CACHEMONEY, and a unique variant of POWBAT to establish a foothold in a target environment. During privilege escalation, freely available tools such as Mimikatz and Ncrack have been observed, in addition to legitimate tools such as Windows Credential Editor and ProcDump. Internal reconnaissance has been performed using custom scripts

How to Identify Techniques?

Use the search
feature on
attack.mitre.org.



How to Identify Techniques?

ATT&CK Powered Suit
browser extension.



<https://ctid.io/suit>

The screenshot shows the ATT&CK Powered Suit browser extension interface. At the top, it features the MITRE logo and the text "Center for Threat Informed Defense". Below this is a search bar with the placeholder text "Search ATT&CK..." and the word "elevation" entered. To the right of the search bar are icons for a bookmark, a settings gear, and a "Sign in" button. Below the search bar is a filter section with three columns of toggle switches. The first column contains "Tactics", "Techniques", "Sub-techniques", and "Campaigns". The second column contains "Mitigations", "Software", "Groups", and "Data Sources". The third column contains "Enterprise", "ICS", "Mobile", and "Deprecated". To the right of these toggles is a link "Select all | none". Below the filter section is a message: "Only showing 25 out of 83 matches. Try narrowing down your search." Below this is a search result for "T1548.004 Abuse Elevation Control Mechanism: Elevated Execution with Prompt". The result includes tags "Enterprise" and "subtechnique". The description text states: "...credentials but no checks on the origin or integrity of the program are made. The program calling the API may also load world writable files which can be modified to perform malicious behavior with elevated privileges." At the bottom, it says: "Adversaries may abuse AuthorizationExecuteWithPrivileges to obtain root privileges in order to install malicious software on victims and install persistence mechanisms.[2][3][4] This technique..."

Step 2: Create Threat Actor Block

Operational Intent

APT39's focus on the telecommunications and travel industries suggests intent to perform monitoring, tracking, or surveillance operations against specific individuals, collect proprietary or customer data for commercial or operational purposes that serve strategic requirements related to national priorities, or create additional accesses and vectors to facilitate future campaigns. Government entities targeting suggests a potential secondary intent to collect geopolitical data that may benefit nation-state decision making. Targeting data supports the belief that APT39's key mission is to track or monitor targets of interest, collect personal information, including travel itineraries, and gather customer data from telecommunications firms.



THREAT ACTOR

APT39

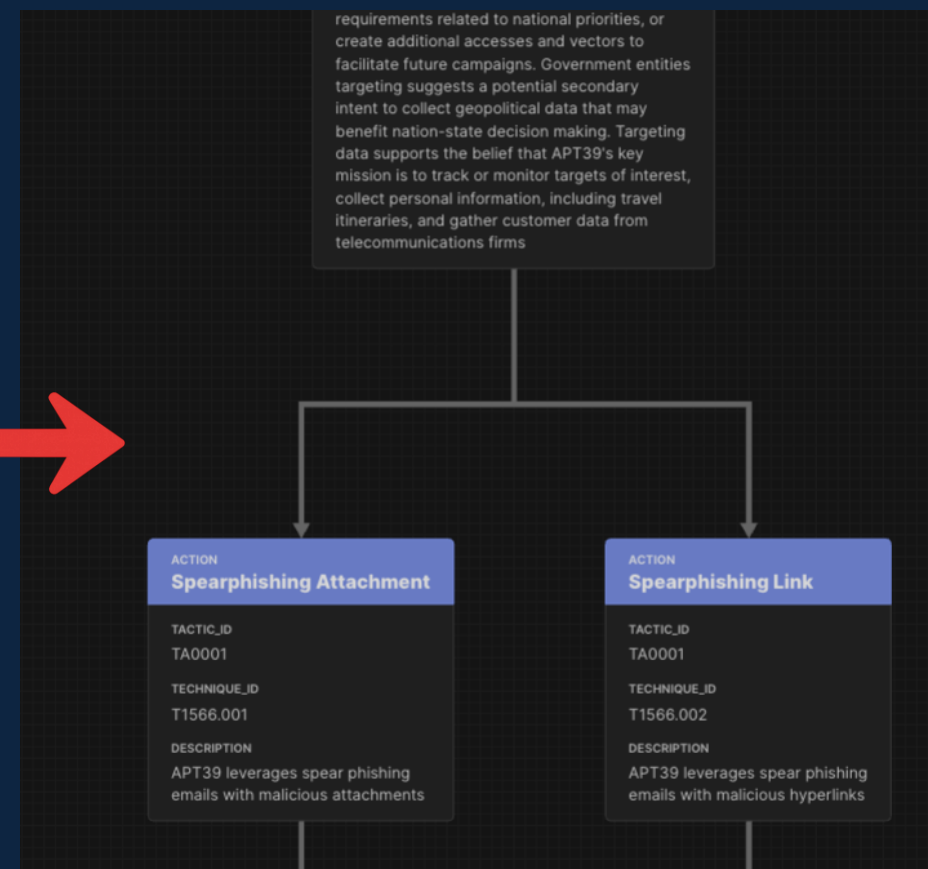
DESCRIPTION

APT39's focus on the telecommunications and travel industries suggests intent to perform monitoring, tracking, or surveillance operations against specific individuals, collect proprietary or customer data for commercial or operational purposes that serve strategic requirements related to national priorities, or create additional accesses and vectors to facilitate future campaigns. Government entities targeting suggests a potential secondary intent to collect geopolitical data that may benefit nation-state decision making. Targeting data supports the belief that APT39's key mission is to track or monitor targets of interest, collect personal information, including travel itineraries, and gather customer data from telecommunications firms

Step 3: Add ATT&CK TTPs as Actions

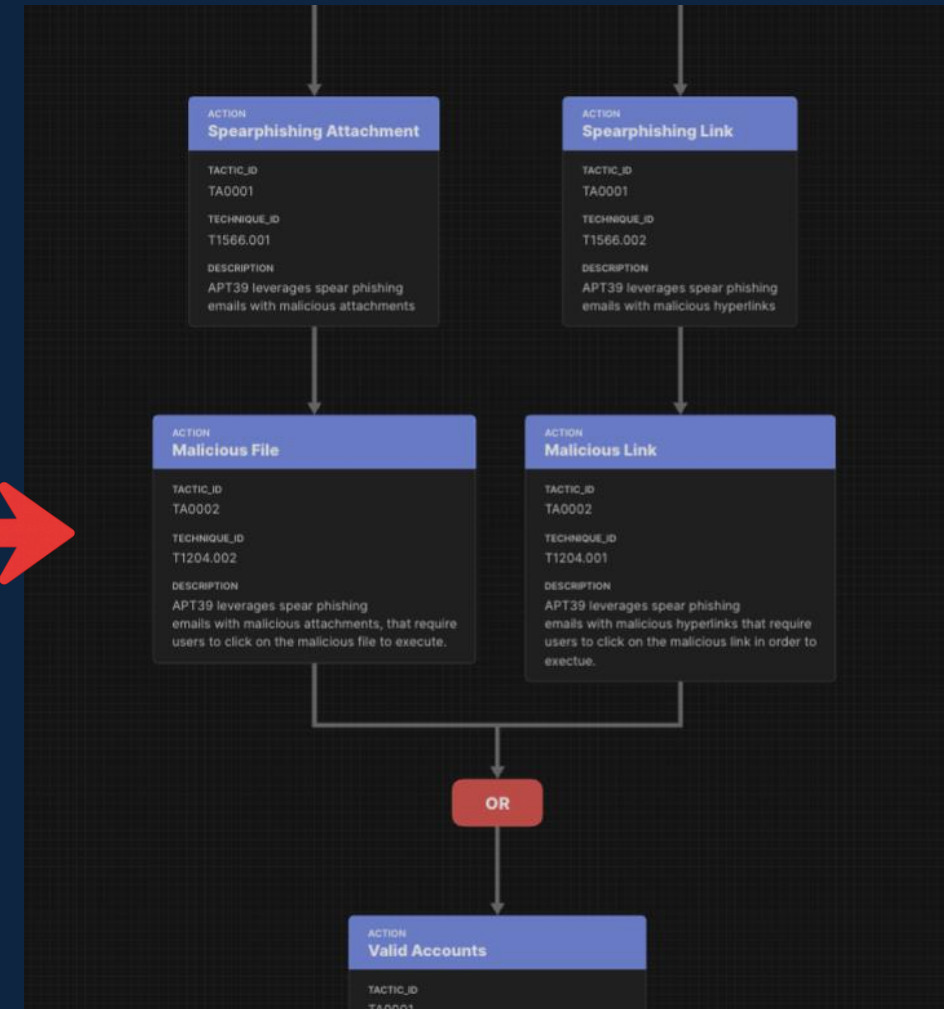
Initial Compromise

For initial compromise, FireEye Intelligence has observed APT39 leverage spear phishing emails with malicious attachments and/or hyperlinks typically resulting in a POWBAT infection. APT39 frequently registers and leverages domains that masquerade as legitimate web services and organizations that are relevant to the intended target.



Step 4: Add in Relationships and Operator Conditions

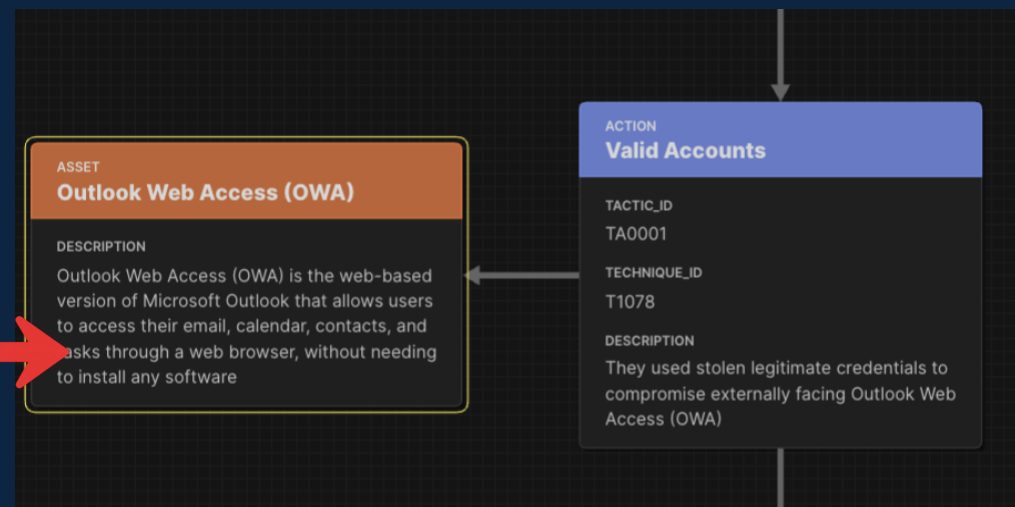
- Using arrows (relationships) to connect actions in a flow helps convey the sequence and logic behind each step
- Operators allow multiple attack paths to converge. In this example, the language from the report implies that if either method of initial access is successful, then the attack can continue.



Step 5: Add Context Objects

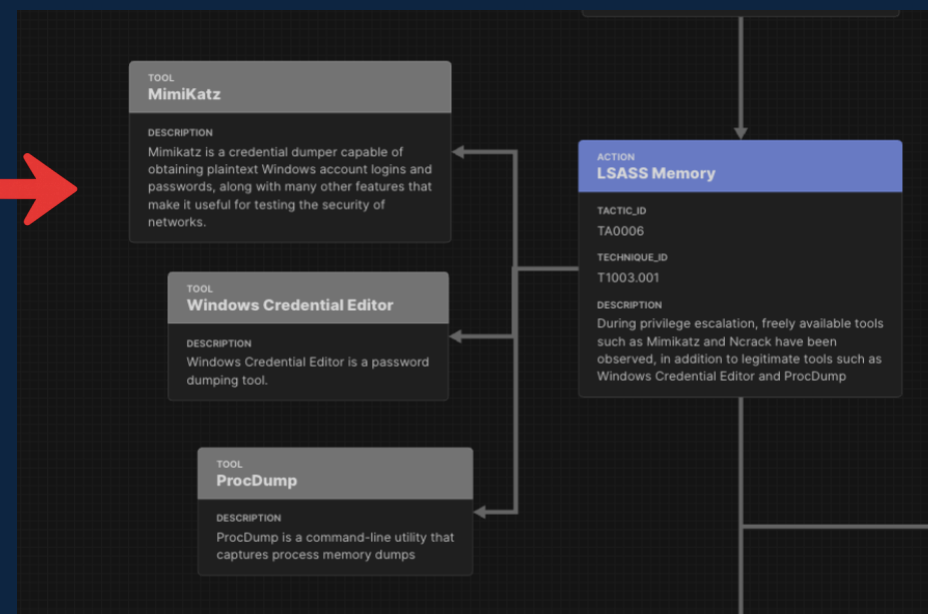
Asset objects:

Furthermore, this group has routinely identified and exploited vulnerable web servers of targeted organizations to **install web shells**, such as ANTAK and ASPXSPY, and used **stolen legitimate credentials** to compromise externally facing Outlook Web Access (OWA) resources.



STIX objects:

Post-compromise, APT39 leverages custom backdoors such as SEAWEED, CACHEMONEY, and a unique variant of POWBAT to establish a foothold in a target environment. During privilege escalation, freely available tools such as **Mimikatz** and **Ncrack** have been observed, in addition to legitimate tools such as **Windows Credential Editor** and ProcDump. Internal reconnaissance has been performed using **custom scrip**



When you're finished...

- Everyone's attack flow will look a little different – there's no “right answer”
- Flow construction *should* be based on the intended audience



Let's Build a Flow!



ctid.io/workshop



A screenshot of a GitHub repository page for 'center-for-threat-informed-defense' with the path 'worksh...'. The 'Wiki' tab is selected. The page title is 'Home', and it shows 'Mark E. Haase edited this page now · 21 revisions'. The main heading is 'CTID Workshop Materials'. Below it, a text block says 'This wiki contains materials used for the Center for Threat-Informed Defense trainings and workshops. Select your event in the pane to the right.' There is a dashed box with a plus icon and the text 'Add a custom footer'. On the right side, there is a 'Pages' sidebar with 8 items. The item 'EU ATT&CK 2025' is circled in red. The sidebar also includes a search bar and a list of other pages like 'APAC ATT&CK - Apr 2024', 'ATT&CKcon 5.0 Oct 2024', 'Build Robust Defenses', 'FS-ISAC 2024 Americas Fall Summit', 'Individual Contributors', and 'INFORM Your Defense'.

End of Section 4

Agenda

- 1 – Introduction to Attack Flow
- 2 – Tagging Techniques in Narrative Reports

Break

- 3 – Using Attack Flow Builder
- *Lightning Talk*
- 4 – Building An Attack Flow

Break

- *Lightning Talk*
- 5 – Attack Flow 3 Preview
- *Lightning Talk*
- 6 – Visualization