

Attack Flow Training: 5 – What's New in v3?

Online Training

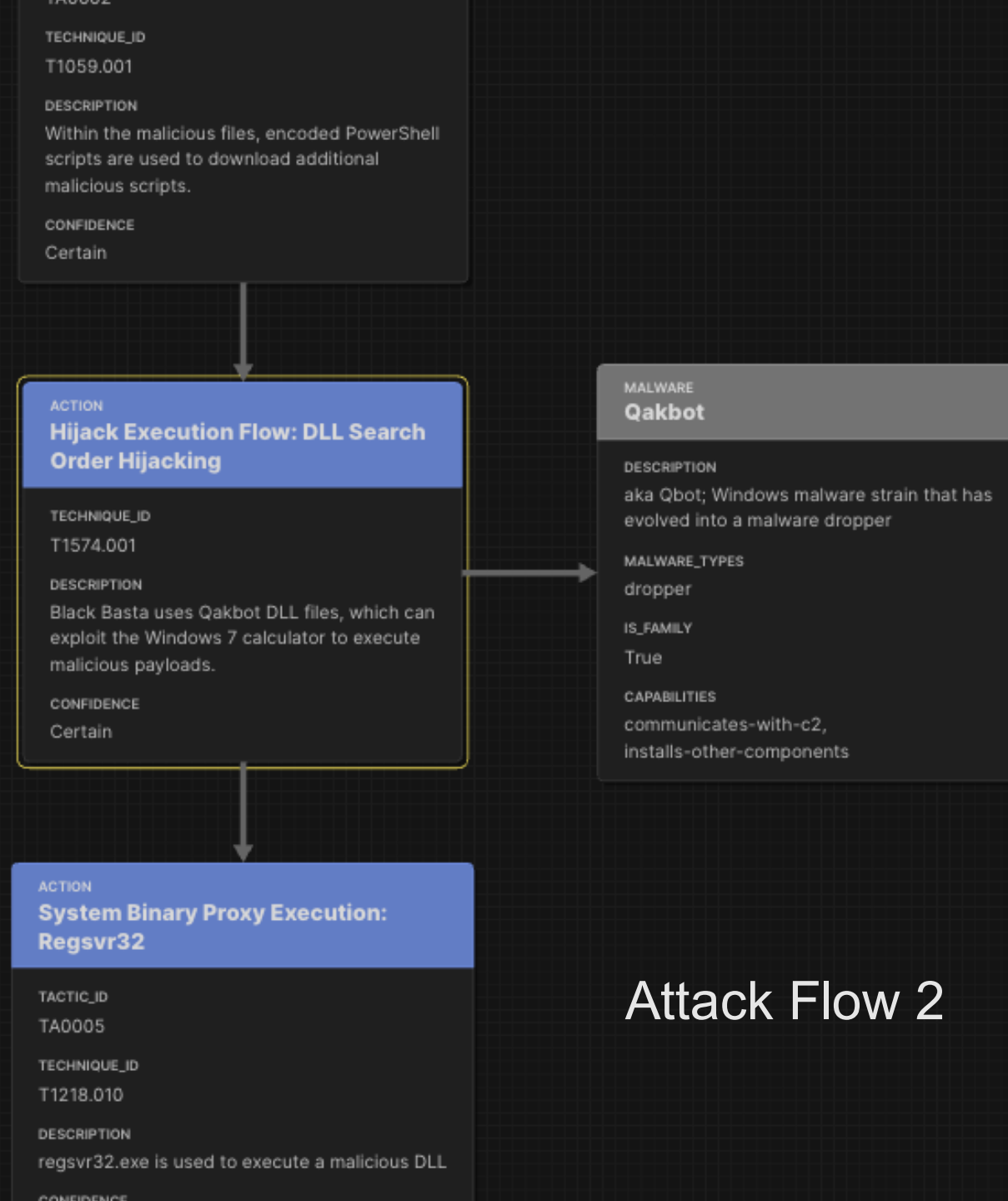


Agenda

- 1 – Introduction to Attack Flow
- 2 – Using Attack Flow Builder
- 3 – Building An Attack Flow
- 4 – Visualization
- 5 – What's New in V3?

New Color Palette & Animations

- Refined color palette
- Subtle animations for item selection (*animation can be turned off*).



Attack Flow 2

New Color Palette & Animations

- Refined color palette with higher contrast and improved readability
- Subtle animations for item selection (*animation can be turned off*).

TECHNIQUE ID
T1059.001

DESCRIPTION
Within the malicious files, encoded PowerShell scripts are used to download additional malicious scripts.

CONFIDENCE
Certain

ACTION
Hijack Execution Flow: DLL Search Order Hijacking

TECHNIQUE ID
T1574.001

TECHNIQUE REF
attack-pattern--2fee9321-3e71-4cf4-af24-d4d40d355b34

DESCRIPTION
Black Basta uses Qakbot DLL files, which can exploit the Windows 7 calculator to execute malicious payloads.

CONFIDENCE
Certain

ACTION
System Binary Proxy Execution: Regsvr32

TACTIC ID
TA0005

TECHNIQUE ID
T1218.010

DESCRIPTION

MALWARE
Qakbot

DESCRIPTION
aka Qbot; Windows malware strain that has evolved into a malware dropper

MALWARE TYPES
dropper

IS FAMILY
True

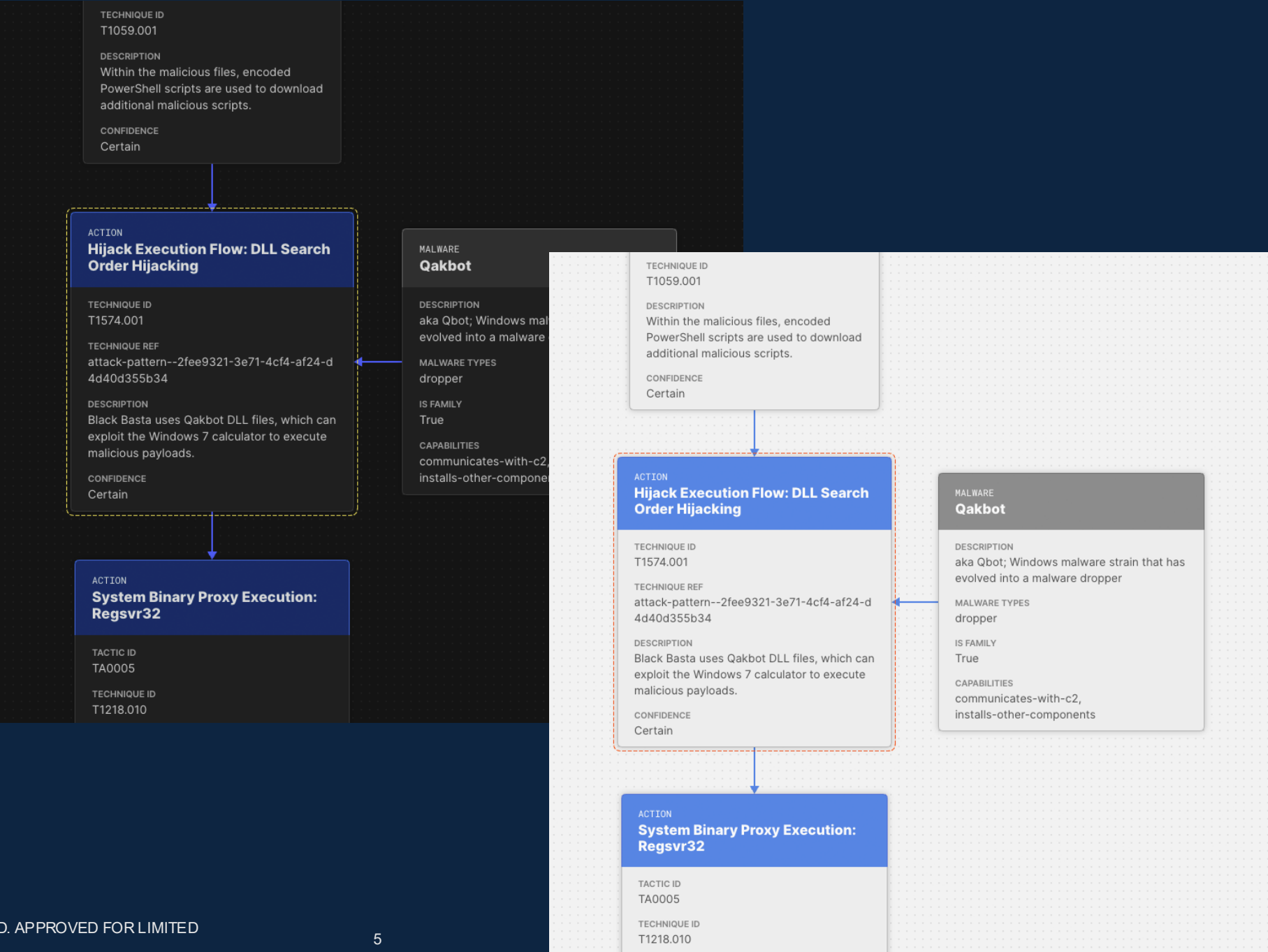
CAPABILITIES
communicates-with-c2,
installs-other-components

Attack Flow 3

Dark or Light Mode

Select the mode that you prefer for work.

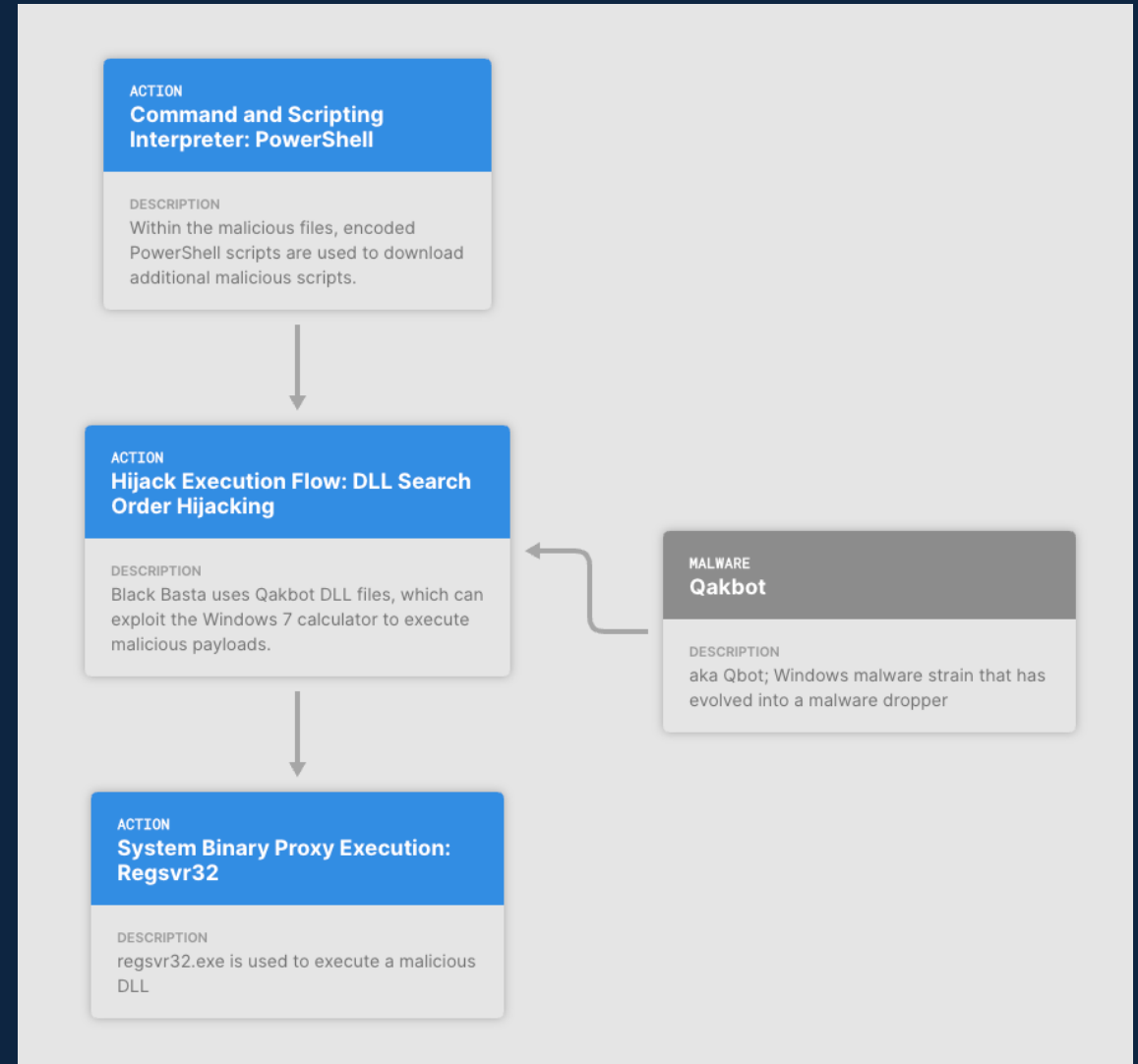
This setting also affects exports; more professional aesthetic for presentations.



Blog Mode

A new visualization option that provides a stylized representation of the flow, suitable for use in presentations, blogs, etc.

It also has an interactive “read-only” mode for embedding in web pages.



Smart Lines

- Attack Flow 2 lines always have two bends, which is awkward in some scenarios.
- Attack Flow 3 has new line types with one bend – and it automatically chooses the best line type for you.

Attack Flow 2



Smart Lines

- Attack Flow 2 lines always have two bends, which is awkward in some scenarios.
- Attack Flow 3 has new line types with one bend – and it automatically chooses the best line type for you.

ACTION Hijack Execution Flow: DLL Search Order Hijacking

TECHNIQUE ID
T1574.001

TECHNIQUE REF
attack-pattern--2fee9321-3e71-4cf4-af24-d
4d40d355b34

DESCRIPTION
Black Basta uses Qakbot DLL files, which can exploit the Windows 7 calculator to execute malicious payloads.

CONFIDENCE
Certain

MALWARE Qakbot

DESCRIPTION
aka Qbot; Windows malware strain that has evolved into a malware dropper

MALWARE TYPES
dropper

IS FAMILY
True

CAPABILITIES
communicates-with-c2,
installs-other-components

Attack Flow 3

ACTION System Binary Proxy Execution: Regsvr32

TACTIC ID
TA0005

TECHNIQUE ID
T1218.010

DESCRIPTION
regsvr32.exe is used to execute a malicious DLL

CONFIDENCE
Certain

Smart Grid

In v3, the grid is de-emphasized and subtler.

ACTION

Hijack Execution Flow: DLL Search Order Hijacking

TECHNIQUE_ID

T1574.001

DESCRIPTION

Black Basta uses Qakbot DLL files, which can exploit the Windows 7 calculator to execute malicious payloads.

CONFIDENCE

Certain

Attack
Flow 2

Smart Grid

In v3, the grid is de-emphasized and subtler.

ACTION

Hijack Execution Flow: DLL Search Order Hijacking

TECHNIQUE ID

T1574.001

DESCRIPTION

Black Basta uses Qakbot DLL files, which can exploit the Windows 7 calculator to execute malicious payloads.

CONFIDENCE

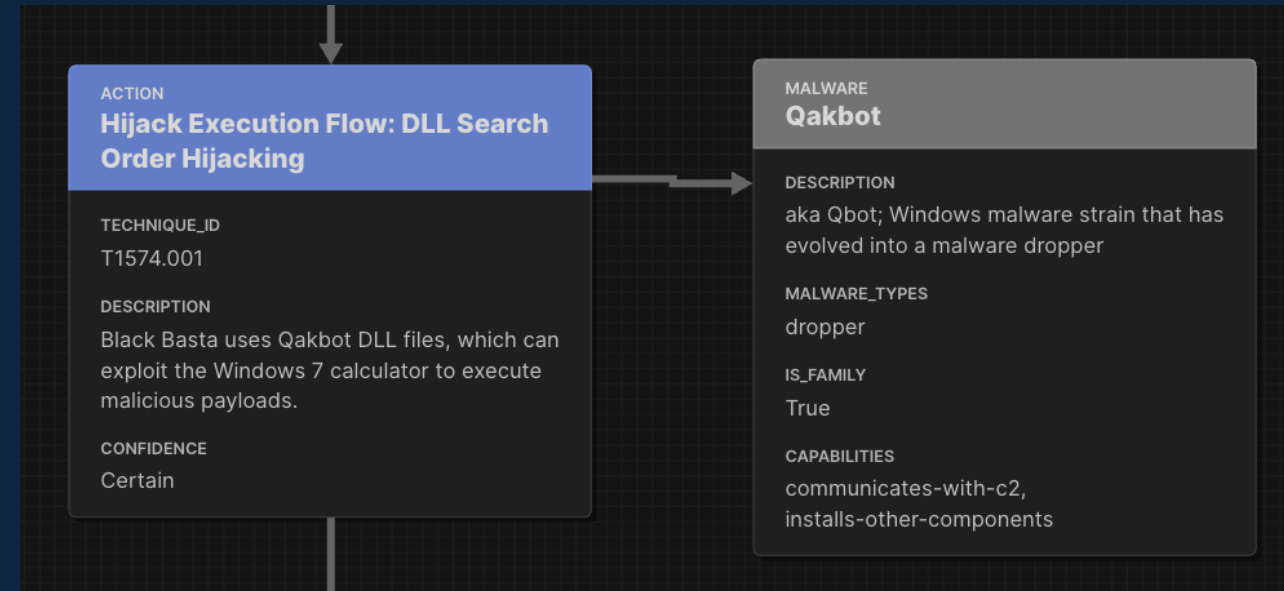
Certain

Attack
Flow 3

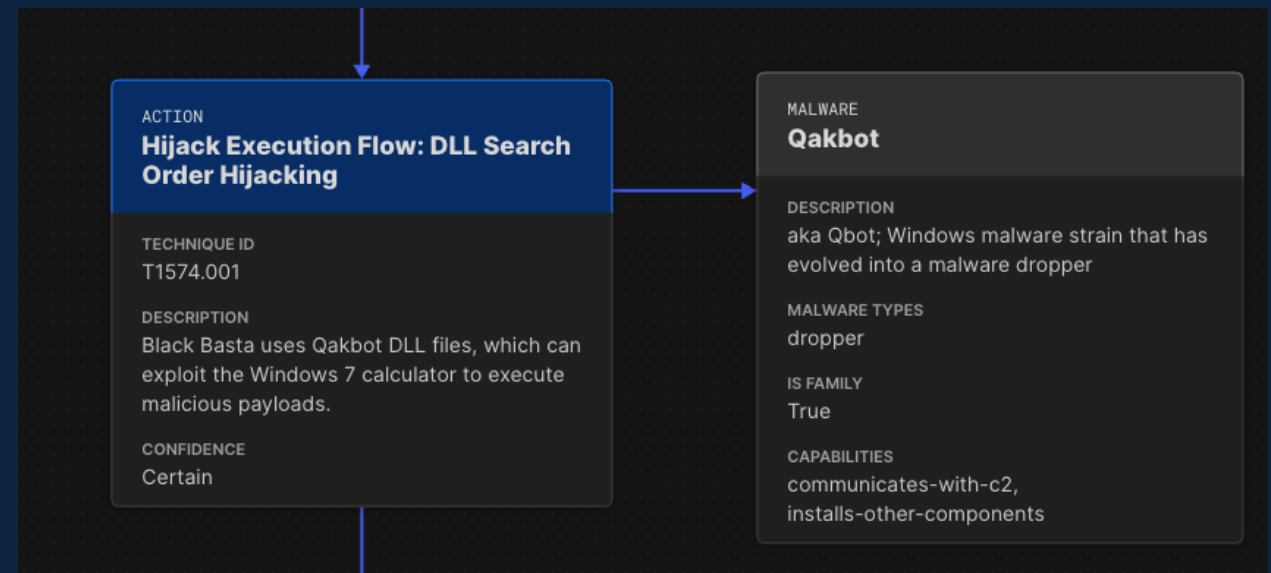
Smart Grid

The new, smarter grid avoids situations where lines cannot be made straight.

Attack Flow 2



Attack Flow 3



Item Insertion

- In Attack Flow 3, drag an item onto a line to insert into the middle of that line.

ACTION
**Command and Scripting
Interpreter: PowerShell**

TACTIC ID
TA0002

TECHNIQUE ID
T1059.001

DESCRIPTION
Within the malicious files, encoded
PowerShell scripts are used to download
additional malicious scripts.

CONFIDENCE
Certain

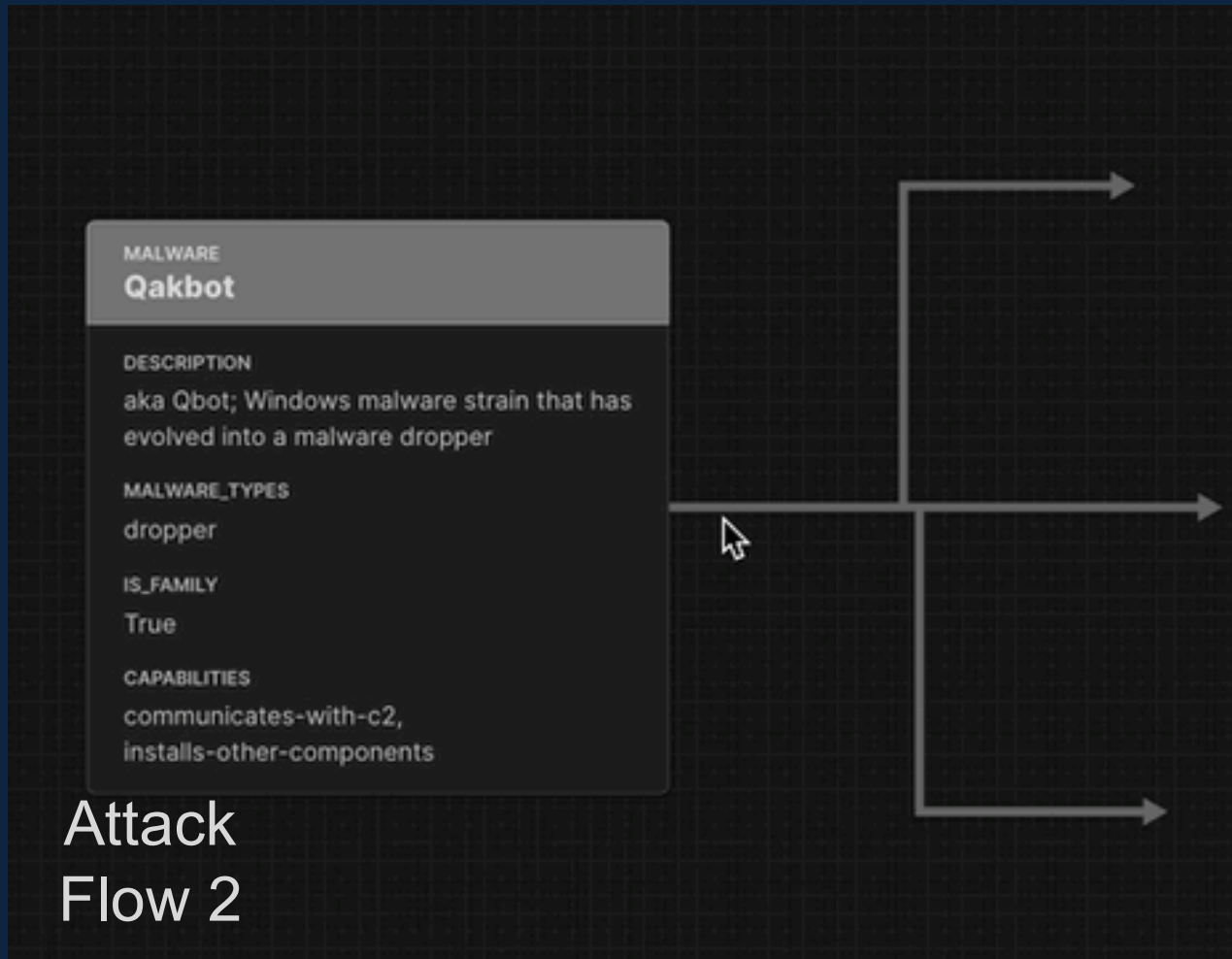
Attack
Flow 3

MALWARE
Qakbot

DESCRIPTION

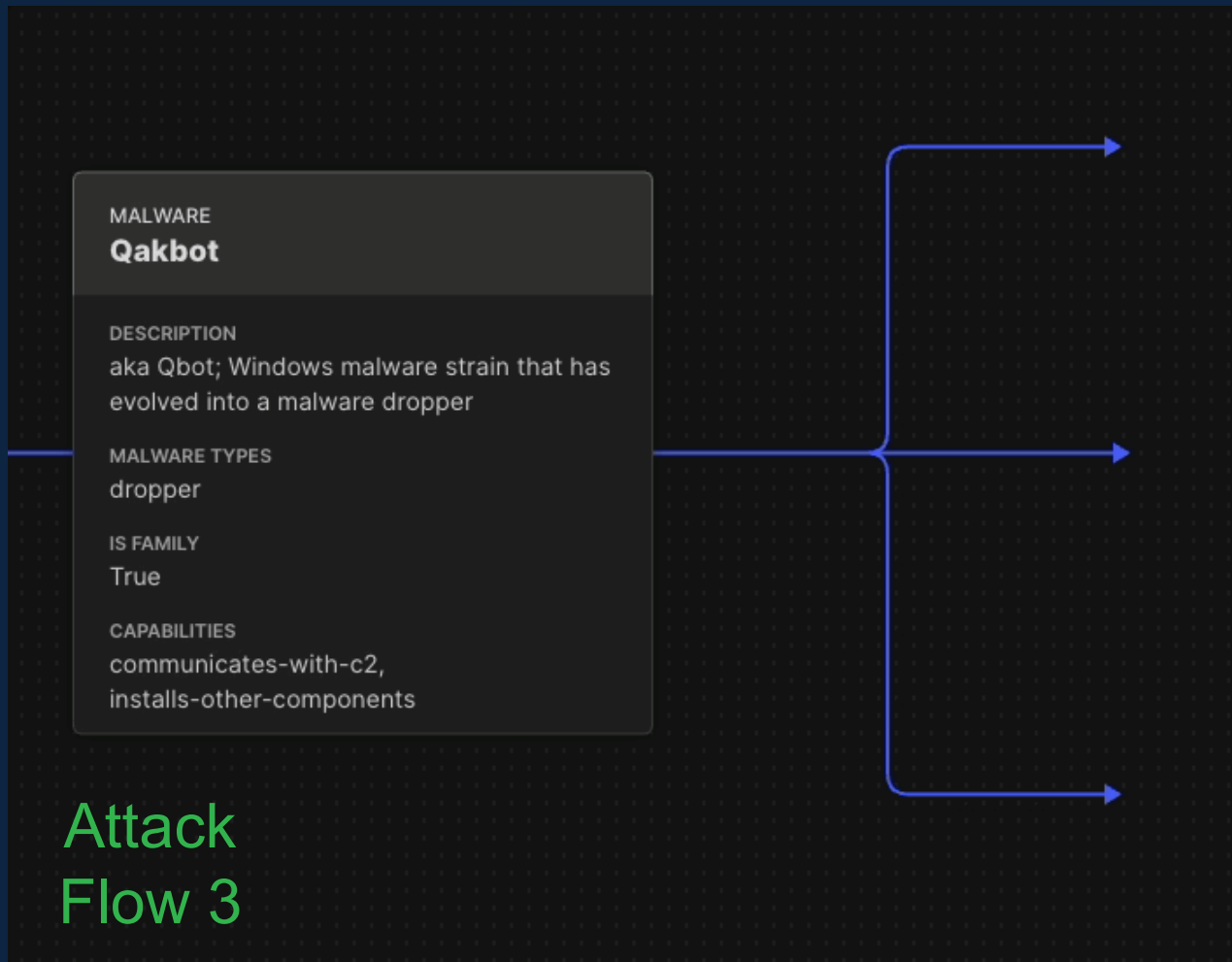
Drag Multiple Anchors

- In Attack Flow 3, you can hold down the CTRL key to drag multiple lines simultaneously.



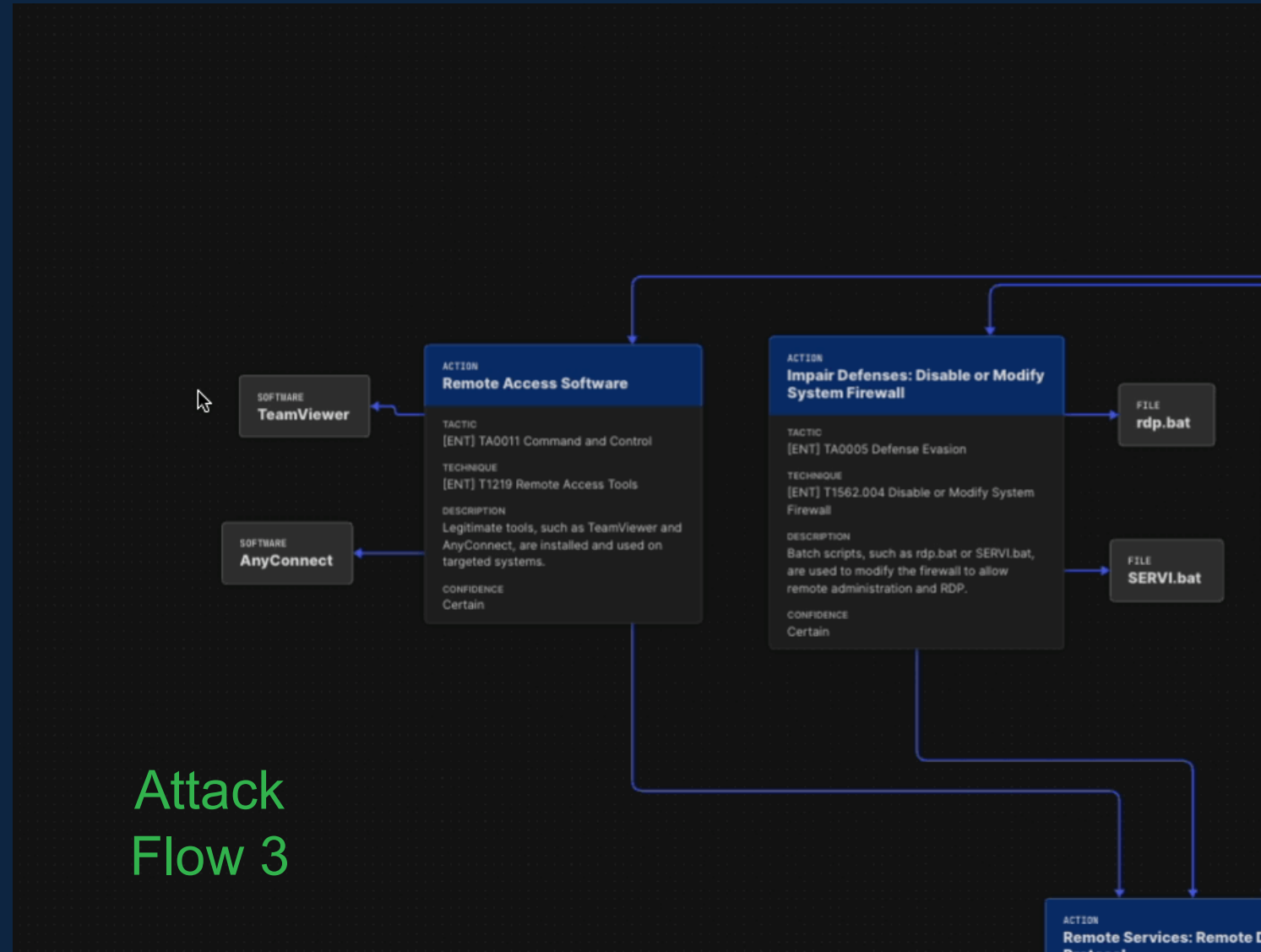
Drag Multiple Anchors

- In Attack Flow 3, you can hold down the CTRL key to drag multiple lines simultaneously.



Rectangle Selection

In Attack Flow 3, hold down the ALT or OPTION key to select multiple items with a rectangle.



Timestamps

- User experience: timestamps are easier to enter and display more compactly
- Localization: timestamps display in your browser's locale.
- Timezones: timestamps can be entered in any timezone.

Attack Flow 2

Execution Start

Nov 21, 2024 - 12:14:00

Execution End

MM / DD / YYYY HH : mm : ss Z

ACTION

Hijack Execution Flow: DLL Search Order Hijacking

TECHNIQUE_ID

T1574.001

DESCRIPTION

Black Basta uses Qakbot DLL files, which can exploit the Windows 7 calculator to execute malicious payloads.

CONFIDENCE

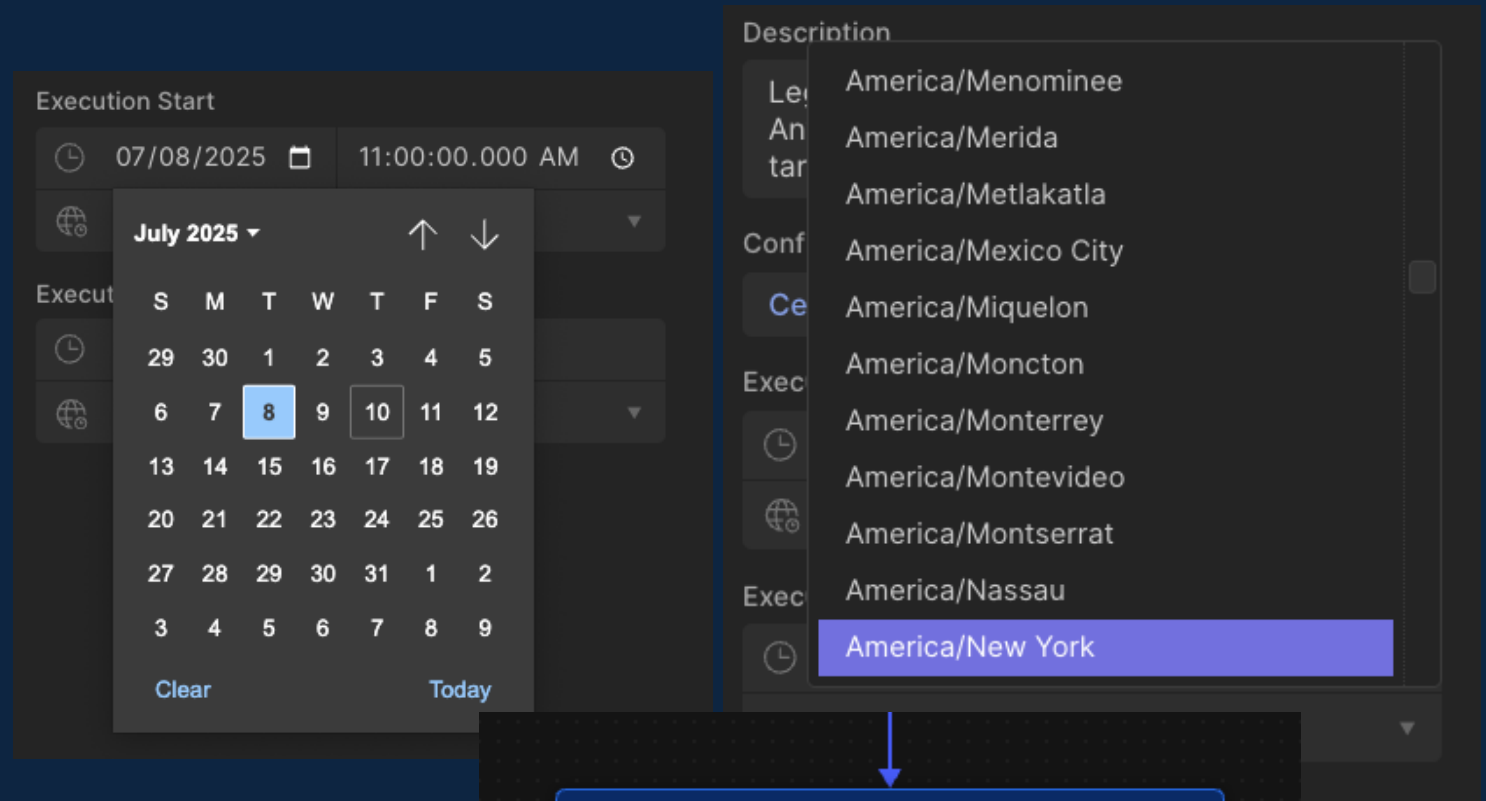
Certain

EXECUTION_START

Thu Nov 21 2024 07:14:00 GMT-0500 (Eastern Standard Time)

Timestamps

- User experience: timestamps are easier to enter and display more compactly
- Localization: timestamps display in your browser's locale.
- Timezones: timestamps can be entered in any timezone.



Attack Flow 3

ACTION
Hijack Execution Flow: DLL Search Order Hijacking

DESCRIPTION
Black Basta uses Qakbot DLL files, which can exploit the Windows 7 calculator to execute malicious payloads.

CONFIDENCE
Certain

EXECUTION START
8/5/2025, 11:00 PM +01:00

Import STIX Bundle

ACTION

Web Protocols

TACTIC ID

TA0011 Command and Control

TECHNIQUE ID

T1071.001 Web Protocols

DESCRIPTION

The payload beacons out to multiple IP addresses for C2.

Create a flow

```
{} ip_loc.json x
Users > mhaase > Downloads > {} ip_loc.json
1
2  {
3    "type": "bundle",
4    "id": "bundle--c8e9f7e2-d4d8-46",
5    "spec_version": "2.1",
6    "created": "2025-06-27T17:06:02",
7    "modified": "2025-06-27T17:06:02",
8    "objects": [
9      {
10       "type": "ipv4-addr",
11       "id": "ipv4-addr--06065698-",
12       "spec_version": "2.1",
13       "created": "2025-06-27T17:06:02",
14       "modified": "2025-06-27T17:06:02",
15       "value": "192.0.2.5"
16     },
17     {
18       "type": "ipv4-addr",
19       "id": "ipv4-addr--ffc732bf-9036-4c95-a7af-49ab0d5b209c",
20       "spec_version": "2.1",
21       "created": "2025-06-27T17:06:02.017Z",
22       "modified": "2025-06-27T17:06:02.017Z",
23       "value": "192.0.2.15"
24     },
25     {
26       "type": "ipv4-addr",
27       "id": "ipv4-addr--4e9fb993-3a0b-4417-8a58-981bf0c1240b",
28       "spec_version": "2.1",
29       "created": "2025-06-27T17:06:02.017Z",
30       "modified": "2025-06-27T17:06:02.017Z",
31       "value": "192.0.2.22"
32     },
33     {
34       "type": "ipv4-addr",
35       "id": "ipv4-addr--4e9fb993-3a0b-4417-8a58-981bf0c1240b",
36       "spec_version": "2.1",
37       "created": "2025-06-27T17:06:02.017Z",
38       "modified": "2025-06-27T17:06:02.017Z",
39       "value": "192.0.2.31"
40     }
41   ]
42 }
```

Import IOCs

ACTION

Web Protocols

TACTIC ID

TA0011 Command and Control

TECHNIQUE ID

T1071.001 Web Protocols

DESCRIPTION

The payload beacons out to multiple IP addresses for C2.

IPV4_ADDR

VALUE

192.0.2.5

IPV4_ADDR

VALUE

192.0.2.15

IPV4_ADDR

VALUE

192.0.2.22

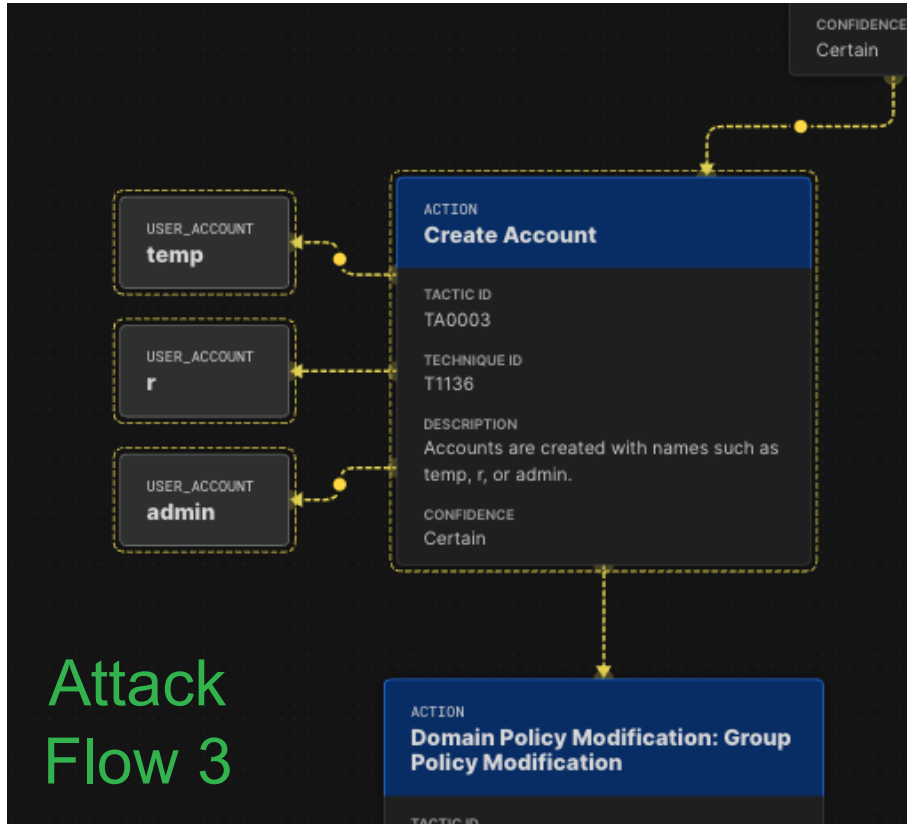
IPV4_ADDR

VALUE

192.0.2.31

Added to flow

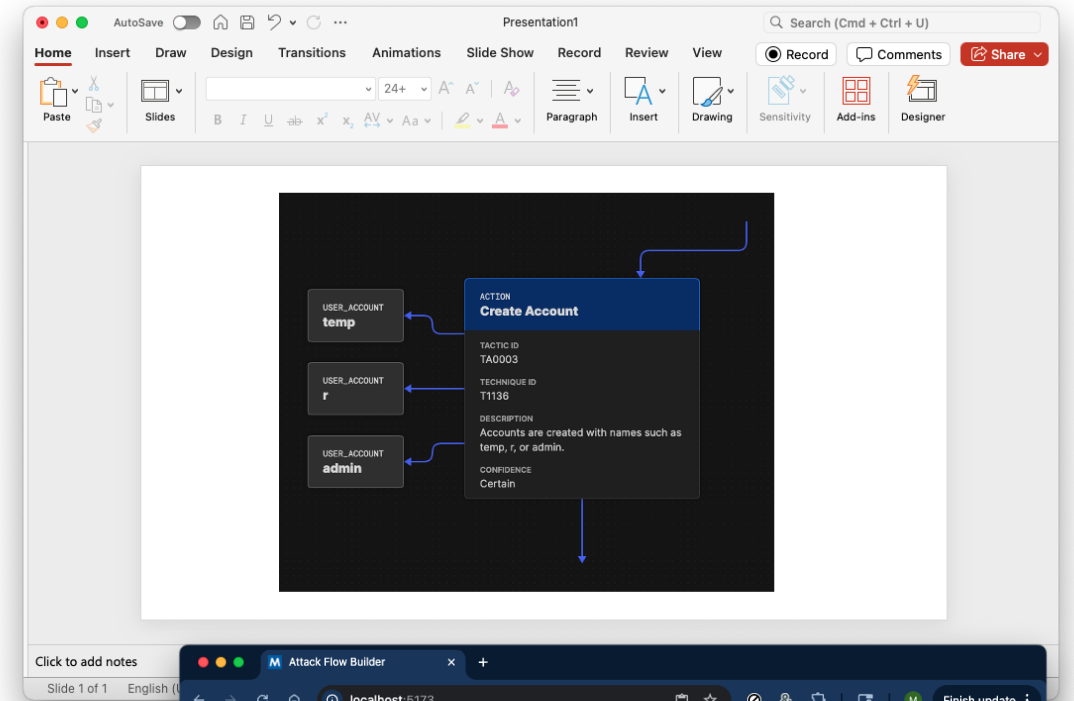
Copy/Paste



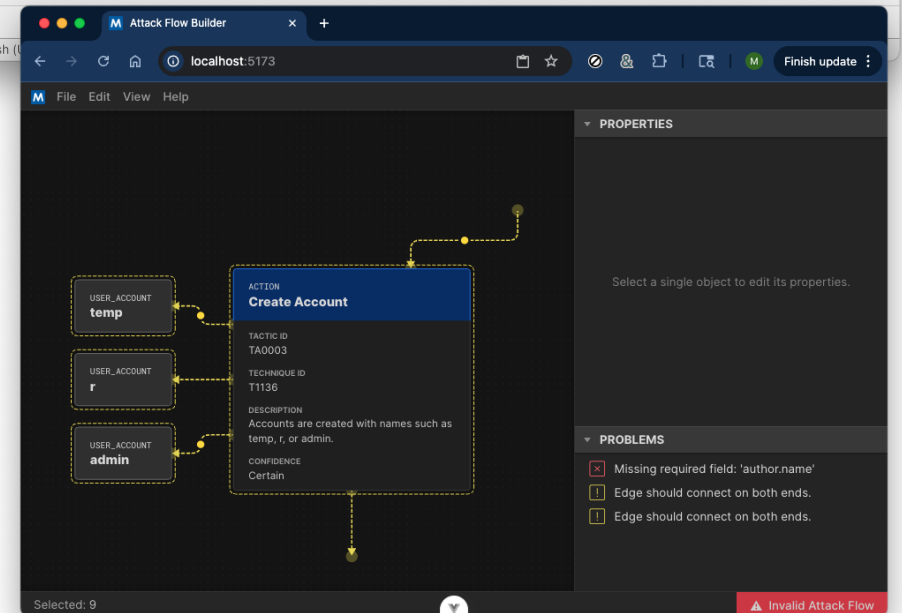
Attack
Flow 3

Select nodes and do
Edit→Copy

Paste image
into any app...



...or into
another flow!



Usage Guides

- 3 usage guides:
 - Cyber Threat Intelligence (CTI)
 - Defensive Posture
 - Adversary Emulation & Red Teaming
- Summarizes insights from our members and their experiences with Attack Flow.
- Includes practical examples in each section to demonstrate how to map data to flows—and explain the rationale behind each step.

The screenshot displays the MITRE Center for Threat Informed Defense website. The main navigation bar includes the MITRE logo and the text 'Center for Threat Informed Defense'. The page title is 'ATTACK FLOW V3.0.0'. The left sidebar contains a search bar and a 'CONTENTS' menu with links to Overview, Introduction, Example Flows, Builder, Usage Guides, Best Practices, Cyber Threat Intelligence, Defensive Posture, Red Teaming, Visualization, Language, and Developers. The main content area is titled 'Mapping CTI Reports to ATT&CK Techniques' and includes a sub-section 'Open-Source Report Selection'. The text explains the importance of selecting high-quality sources for creating attack flows. A 'Key Takeaways for Selecting a Report' box lists four points: reports should be transparent, originate from credible vendors, provide current information, and make it easy to identify information gaps. The right sidebar, titled 'ON THIS PAGE', lists links to 'Mapping CTI Reports to ATT&CK Techniques', 'Examples of Reports to Avoid', 'Examples of Reports to Use', and 'Example Technique Mapping'. Below the main content, there is a 'Builder' section with a 'Usage Guides' menu and a 'Defensive Posture' section. A code block shows an XML snippet for an event, detailing system information, process details, and user information.

cyber-threat-intelligence.github.io/attack-flow/usage_guides/cyber-threat-intel/

ATTACK FLOW V3.0.0

MITRE | Center for Threat Informed Defense

Search docs

CONTENTS

- Overview
- Introduction
- Example Flows
- Builder
- Usage Guides
- Best Practices
- Cyber Threat Intelligence
- Defensive Posture
- Red Teaming
- Visualization
- Language
- Developers

Mapping CTI Reports to ATT&CK Techniques

Open-Source Report Selection

If you choose to use an open-source report to create an attack flow, it is important to assess the strengths and weaknesses of the report in order to establish a confidence level in its data and assessments. Factors affecting source quality include the manner of data collection, the level of source access to the data, report completeness, and the age and currency of the information. In addition to extracting the technical details, it is also beneficial to construct the victimology of the attack from the reports, as its inclusion will allow any reader to quickly gauge the scope and applicability of the flow to their own organization. It is important to use high-quality sources, because they will support the credibility of your flow and provide an accurate portrayal of the threat, which may be used to inform decisions on defense and resource prioritization.

Important

Key Takeaways for Selecting a Report

- Reports should be transparent about where the data originates and provide a technically competent overview of an incident.
- Reports should originate from a credible vendor with a track record of accurate reporting and first-hand analysis of the incident in question.
- Reports should provide the most current information on the malware or breach.
- Reports should make it easy to identify any information gaps. Use multiple sources to address gaps and corroborate the data.

ON THIS PAGE

- Cyber Threat Intelligence
- Mapping CTI Reports to ATT&CK Techniques
- Examples of Reports to Avoid
- Examples of Reports to Use
- Example Technique Mapping

Builder

- Usage Guides
- Best Practices
- Cyber Threat Intelligence
- Defensive Posture
- Red Teaming
- Visualization
- Language
- Developers

```
<System>
  <Provider Name="Microsoft-Windows-Sysmon" Guid="{577038
  <EventID>1</EventID>
  <TimeCreated SystemTime="2025-02-25T15:25:37.456Z"/>
  <Execution ProcessID="7852" ThreadID="3152"/>
  <Computer>COMP123</Computer>
</System>
<EventData>
  <Data Name="UtcTime">2025-02-25T15:25:37.456Z</Data>
  <Data Name="ProcessGuid">{b2f8d0d7-c62f-4e4b-9a3c-38d74
  <Data Name="ProcessId">7852</Data>
  <Data Name="Image">C:\Windows\Temp\mimikatz.exe</Data>
  <Data Name="CommandLine">mimikatz.exe privilege::debug
  <Data Name="Hashes">MD5=5f66b82558ca92e54e77f216ef4c066
  <Data Name="User">COMP123\JaneAdmin</Data>
  <Data Name="ParentProcessId">3240</Data>
  <Data Name="ParentImage">C:\Windows\System32\cmd.exe</D
  <Data Name="ParentCommandLine">cmd.exe /c mimikatz.exe<
  <Data Name="Description">Adversary executed Mimikatz to
</EventData>
</Event>
```

Center for Threat Informed Defense

THIS PAGE

- Defensive Posture
- Mapping System Data to Attack Flow
- Example Windows Event Logs for Attack Flow
- Event Logs to Flow Diagram
- Post-Flow: Identifying Gaps in Adversary Behaviors
- Supplemental Fields and STIX Object Mappings

End of Section 5