

Agenda

Intro

Attack Flow in action

Before we begin

Attack Flow Components

Problem

Impact Statement

Solution

Outro

About me

- Senior Security Solution Architect – APAC, Splunk a Cisco Company
- Previously worked at – Cisco, Rapid7, McAfee
- Current Specialisation – Threat Detection / Hunting / Intelligence, Security Automation, Machine Learning
- Previous experience – Network Security, Blue Teaming, Malware Engineering
- 20+ years of experience in Security
- Certifications – ISC2, Splunk, Cisco, EC-Council, ISO, etc.
- Publications – IEEE, TechRepublic, Enterprise Executive, US Cybersecurity Magazine, Australian Security Magazine
- Speaking – AISA CyberCon Melbourne & Canberra, CISO Summit, Splunk .confGo, Cisco Live
- Connect with me – share ideas, collaborate on ongoing projects/research, co-authoring opportunities, technical projects

About the project

MITRE

MITRE | ATT&CK[®]

MITRE | Center for Threat
Informed Defense™

Problem



Defenders often track adversary behaviours atomically, focusing on one specific action at a time. This makes it harder to understand adversary attacks and to build effective defences against those attacks

Example - Cryptojacking

Tesla cloud systems exploited by hackers to mine cryptocurrency

Updated: Researchers have discovered that Tesla's AWS cloud systems were compromised for the purpose of cryptojacking.



Written by **Charlie Osborne**, Contributing Writer
Feb. 20, 2018 at 6:00 a.m. PT



Tesla

Tesla's cloud environment has been exploited by threat actors to mine cryptocurrencies, researchers have discovered.

On Tuesday, cloud security firm **RedLock** released the firm's **2018 Cloud Security Trends** report which / security

Strategies for Building a Change-Seeking Culture
Future-ready organizations are taking action
EXPLORE THE INSIGHTS

related

Massive TransUnion breach leaks personal data of 4.4 million customers - what to do
CLICK TO UNMUTE



Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 16 techniques
Active Scanning (10)	Acquire Infrastructure (1)	Drive-by Compromise (1)	Command and Scripting Interpreter (1)	Account Manipulation (2)	Abuse Elevation Control Mechanism (1)	Abuse Elevation Control Mechanism (1)	Adversary-in-the-Middle (1)
Gather Victim Host Information (1)	Compromise Accounts (2)	Exploit Public-Facing Application (1)	Container Administration Command (1)	BTS Jobs (1)	Access Token Manipulation (1)	Access Token Manipulation (1)	Brute Force (1)
Gather Victim Identity Information (1)	Compromise Infrastructure (1)	External Remote Services (1)	Deploy Container (1)	Boot or Login Autostart Execution (1)	Boot or Login Autostart Execution (1)	BITS Jobs (1)	Credentials from Password Stores (1)
Gather Victim Network Information (1)	Develop Capabilities (1)	Hardware Additions (1)	Exploitation for Client Execution (1)	Boot or Login Initialization Scripts (1)	Boot or Login Initialization Scripts (1)	Built Image on Host (1)	Exploitation for Credential Access (1)
Gather Victim Org Information (1)	Establish Accounts (1)	Phishing (1)	Inter-Process Communication (1)	Browser Extensions (1)	Boot or Login Initialization Scripts (1)	Debugger Evasion (1)	Forced Authentication (1)
Phishing for Information (1)	Obtain Capabilities (1)	Replication Through Removable Media (1)	Twilio API (1)	Compromised Client (1)	Create or Modify System Process (1)	Deobfuscate/Decode Files or Information (1)	Forge Web Credentials (1)
Search Closed Sources (1)	Stage Capabilities (1)	Supply Chain Compromise (1)	Scheduled Task/Job (1)	Create Account (1)	Domain Policy Modification (1)	Deploy Container (1)	Input Capture (1)
Search Open Technical Databases (1)		Trusted Relationship (1)	Shared Modules (1)	Create or Modify System Process (1)	Escape to Host (1)	Direct Volume Access (1)	Modify Authentication Process (1)
Search Open Websites/Domains (1)		Valid Accounts (1)	Software Deployment Tools (1)	Event Triggered Execution (1)	Event Triggered Execution (1)	Domain Policy Modification (1)	Multi-Factor Authentication Interception (1)
Search Victim-Owned Websites (1)			System Services (1)	External Remote Services (1)	Exploitation for Privilege Escalation (1)	Execution Guardrails (1)	Multi-Factor Authentication Request Generation (1)
			User Execution (1)	Hijack Execution Flow (1)	Hijack Execution Flow (1)	Exploitation for Defense Evasion (1)	Network Sniffing (1)
			Windows Management Instrumentation (1)	Implant Internal Image (1)	Process Injection (1)	File and Directory Permissions Modification (1)	OS Credential Dumping (1)
				Modify Authentication Process (1)	Scheduled Task/Job (1)	Hide Artifacts (1)	Steal Application Access Token (1)
				Office Application Startup (1)	Valid Accounts (1)	Hijack Execution Flow (1)	Steal or Forge Kerberos Tickets (1)
				Pre-OS Boot (1)		Indicator Removal on Host (1)	Steal Web Session Cookie (1)
				Scheduled Task/Job (1)		Indirect Command Execution (1)	Unsecured Credentials (1)
				Server Software Component (1)		Masquerading (1)	
				Traffic Signaling (1)		Modify Authentication Process (1)	
				Valid Accounts (1)		Modify Cloud Compute Infrastructure (1)	

Atomic attacks & mitigation

```
`sysmon` EventCode=10 TargetImage=*lsass.exe (GrantedAccess=0x1010 OR GrantedAccess=0x1410)
| stats count min(_time) as firstTime max(_time) as lastTime by CallTrace EventID GrantedAccess Guid
Opcode ProcessID SecurityID SourceImage SourceProcessGUID SourceProcessId TargetImage TargetProcessGUID
TargetProcessId UserID dest granted_access parent_process_exec parent_process_guid parent_process_id
parent_process_name parent_process_path process_exec process_guid process_id process_name process_path
signature signature_id user_id vendor_product
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
| `detect_credential_dumping_through_lsass_access_filter`
```



```
index=windows OR index=wineventlog sourcetype=wineventlog
|dedup EventCode
|rex field=EventCodeDescription (?<account_desc>account)
|where EventCodeDescription NOT null AND account_desc NOT null
|table _time dest_nt_domain dest_nt_host src_user EventCode
EventCodeDescription
|rename dest_nt_domain AS Domain dest_nt_host AS Host src_user AS User
```

Realism – Why Attack Flows are important

A single block IS NOT a stopped attack

Attackers persist and try to find other avenues of attack

Alert Fatigue

Too many alerts = alert fatigue

Too many alerts = too much information to parse through

Alert fatigue = relevant information gets ignored

Describing/Mapping adversary behaviour



T1105:
Ingress Tool
Transfer



T1059.001:
Powershell



T1132:
Obfuscated
Files

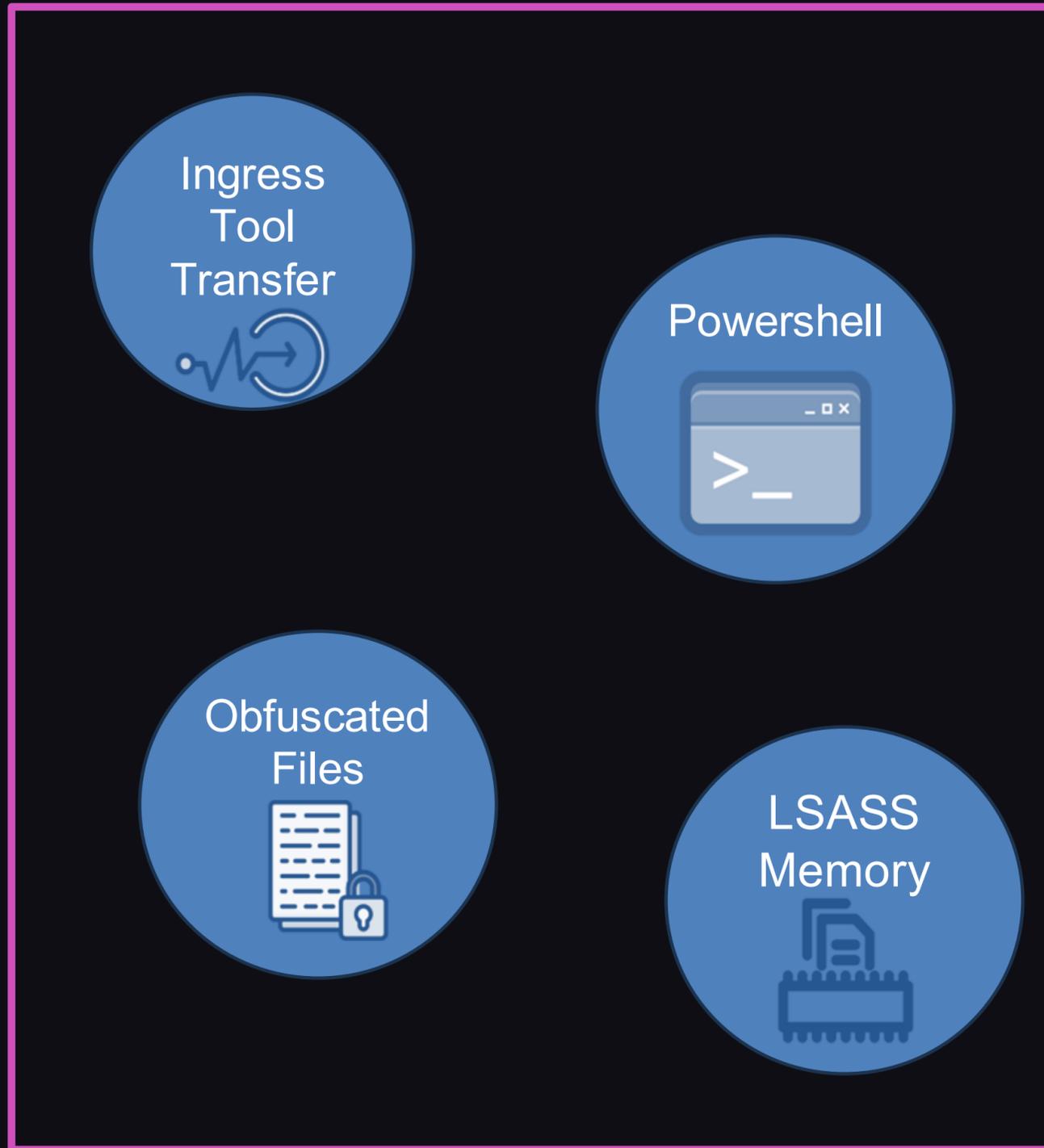


T1003.001:
LSASS
Memory

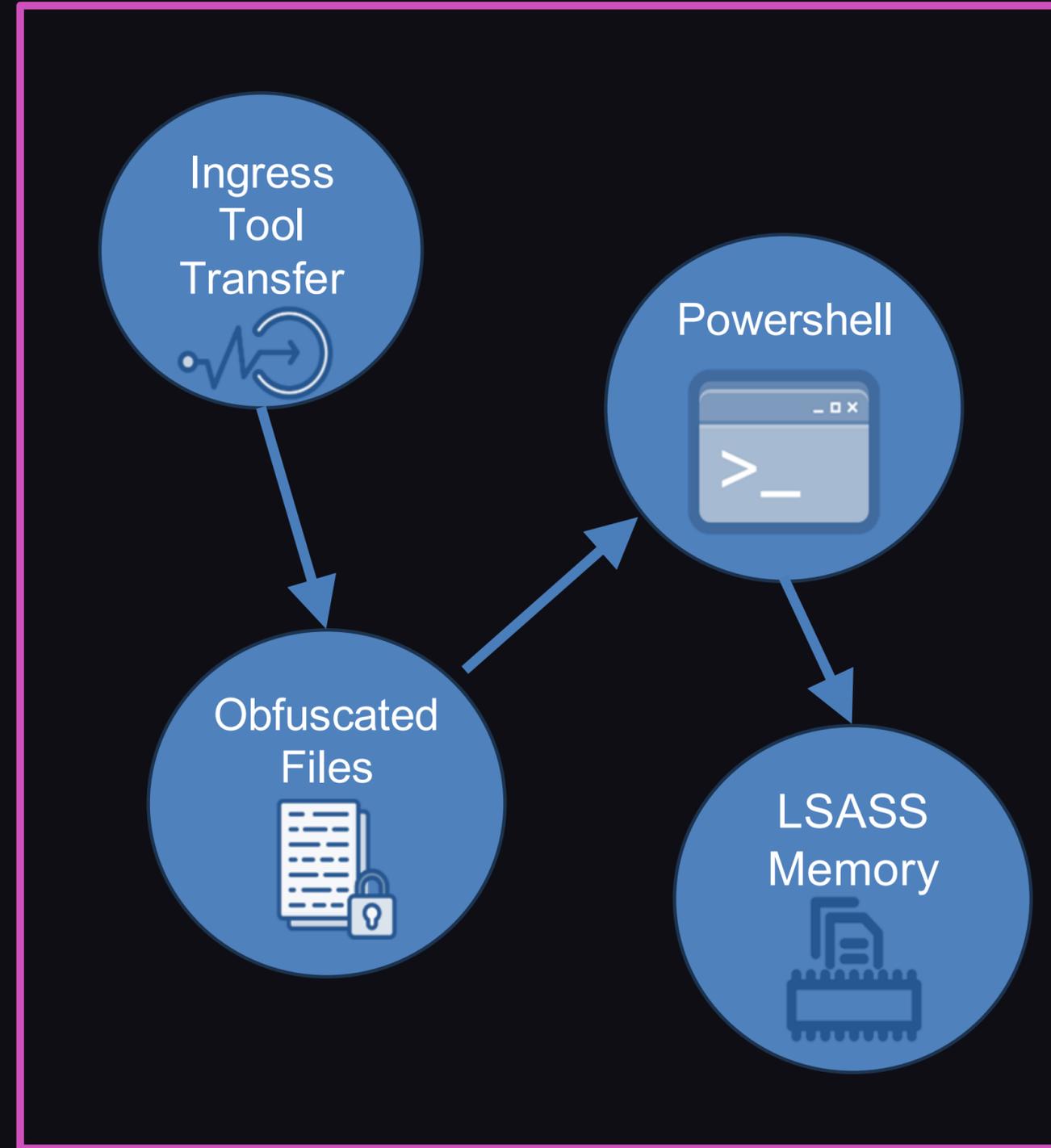


Atomic Behaviours

Describing/Mapping adversary behaviour



Atomic Behaviours



Sequenced Behaviours

Solution

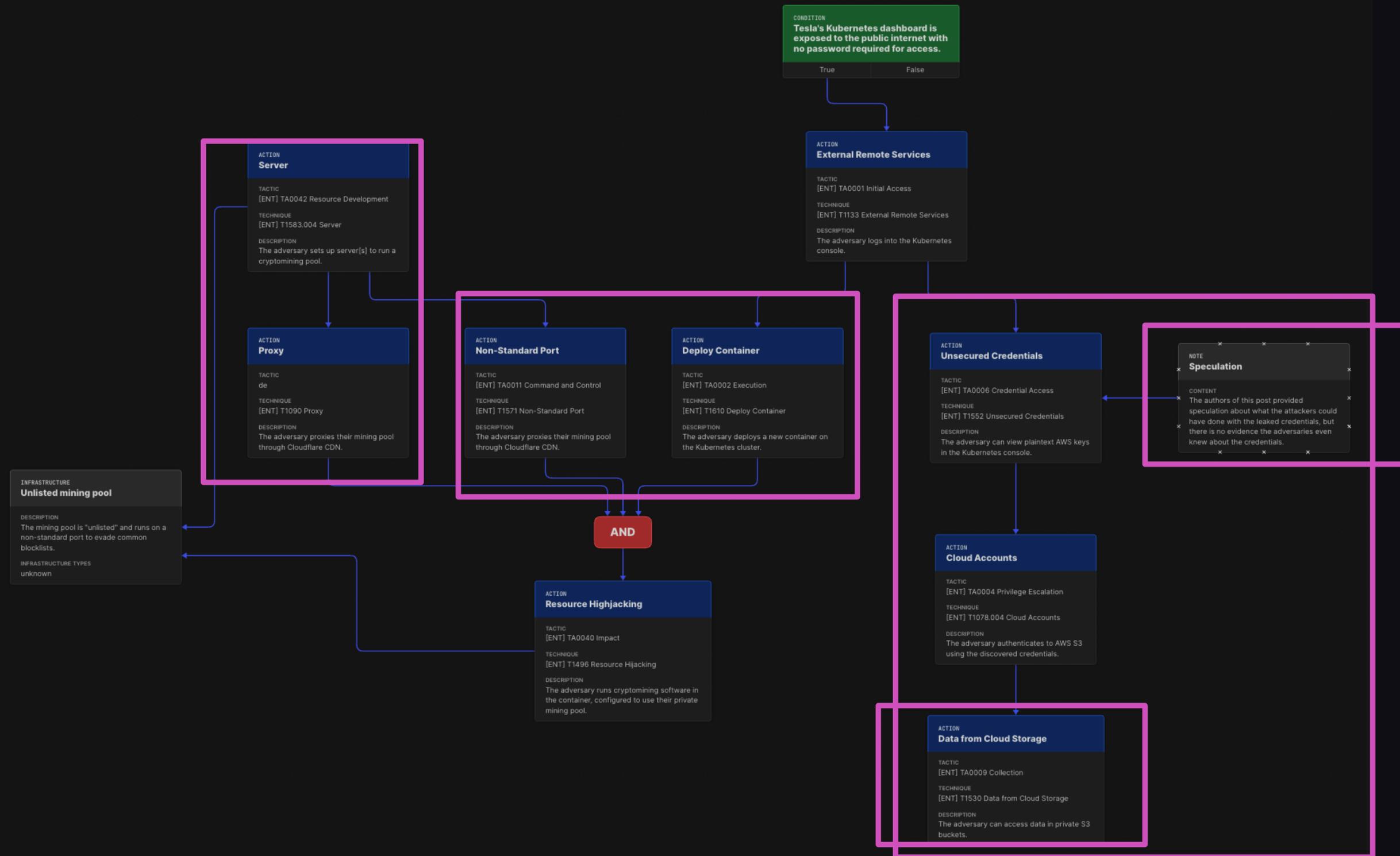


Create a language, and associated tooling, to describe flows of ATT&CK techniques and combine those flows into patterns of behaviour.

Attack Flow

What it is?

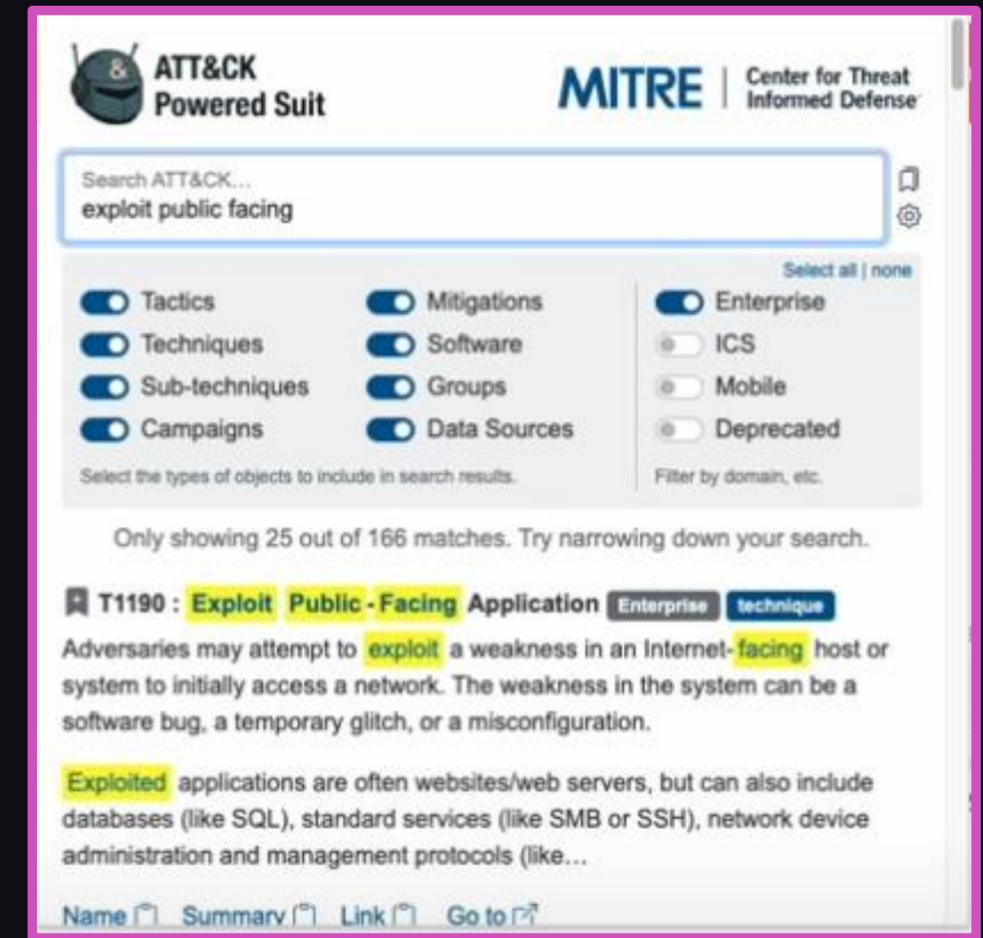
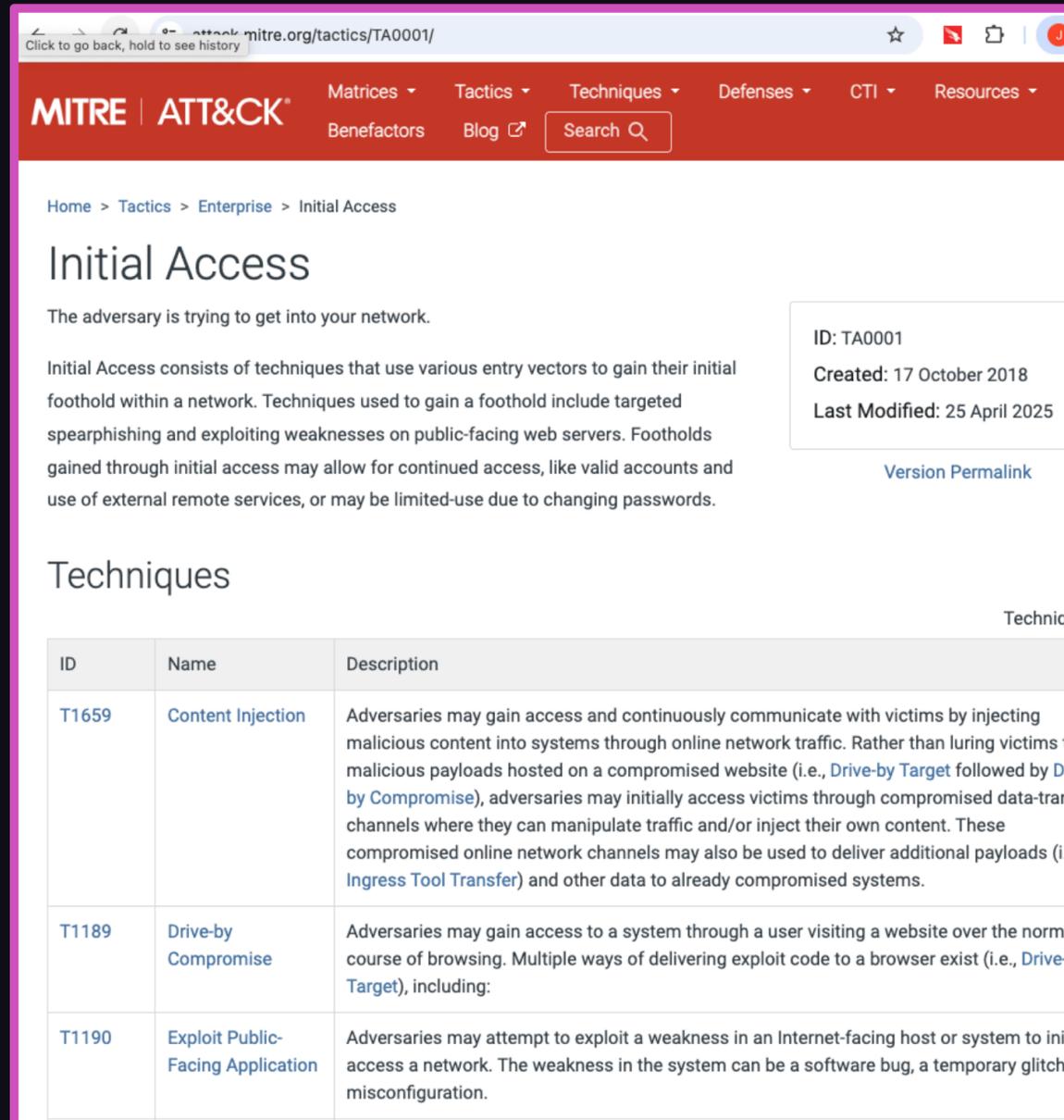
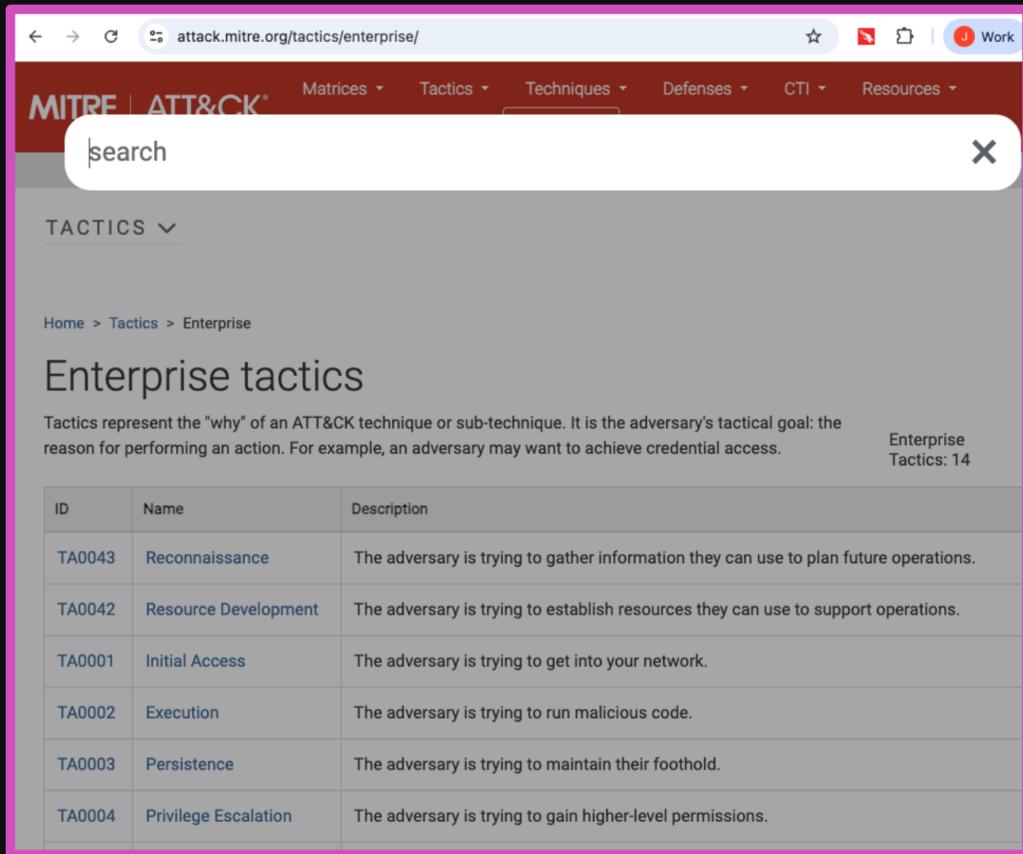
Attack Flow – Tesla Kubernetes Breach



Approach to Flow Building

1. Find appropriate CTI reporting.
2. Annotate the report with TTPs.
3. Create the actions in the flow based on the TTPs.
4. Add additional items for context: IOCs, Assets, etc.

Using Attack Flow for CTI



Browser Extension

attack.mitre.org/tactics/..

Sharepoint Exploit Flow

July 28, 2025 at 12:56 PM

Sharepoint Exploit Flow

<https://www.akamai.com/blog/security-research/sharepoint-vulnerability-rce-active-exploitation-detections-mitigations>

<https://unit42.paloaltonetworks.com/microsoft-sharepoint-cve-2025-49704-cve-2025-49706-cve-2025-53770/>

T0819: Exploit Public-Facing Application

Exploiting the authentication bypass (CVE-2025-49706) - Improper authentication in Microsoft Office SharePoint allows an unauthorized attacker to perform spoofing over a network.

The first step in exploiting CVE-2025-49706 is to send a specially crafted POST request to the endpoint, manipulating the HTTP 'Referer' header. The attacker targets the endpoint value `/_layouts/15/ToolPane.aspx?DisplayMode=Edit&a=/_layouts/15/ToolPane.aspx` with the crafted value `/_layouts/15/SignOut.aspx` to manipulate the system into trusting the request and its payload.

Exploiting the deserialization vulnerability (CVE-2025-49704) - Improper control of generation of code ('code injection') in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.

T1059.001: Command and Scripting Interpreter: PowerShell

Once the authentication bypass is achieved, attackers can exploit the deserialization vulnerability to execute PowerShell code.

Akamai Variant:

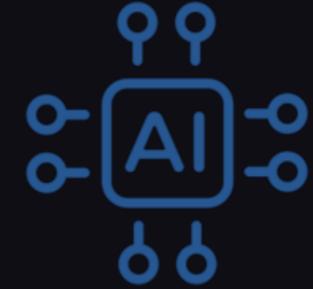
T1505.003: Server Software Component: Web Shell

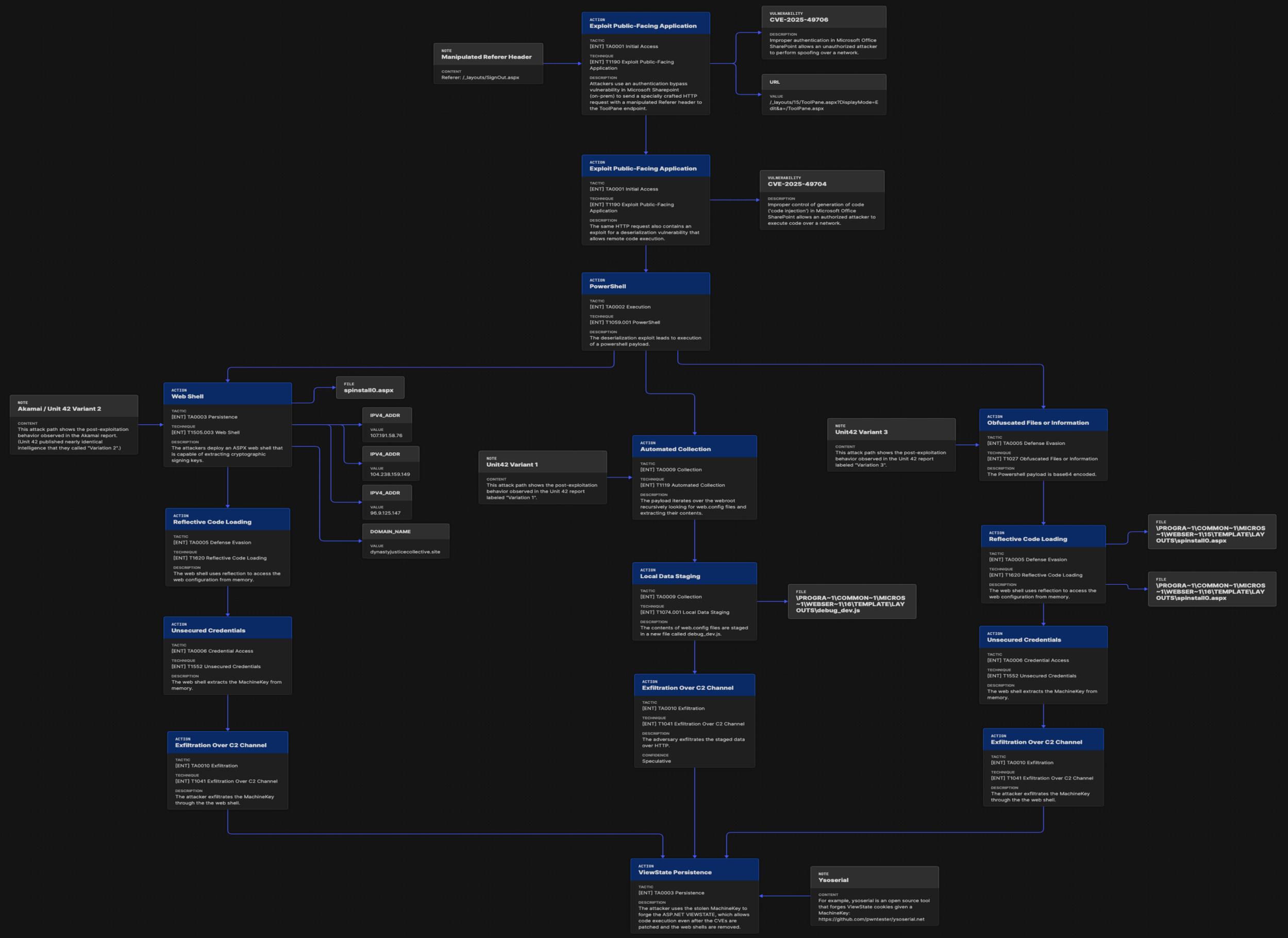
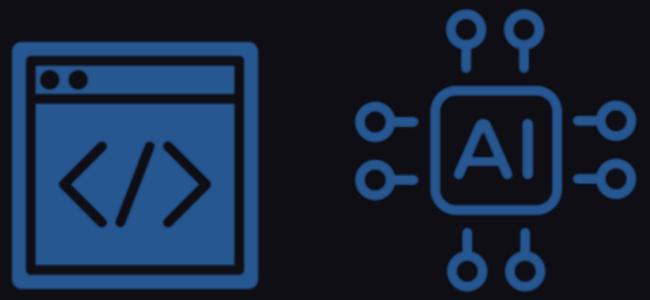
In observed attacks, attackers deployed a malicious second-stage ASPX file designed to extract cryptographic keys that are signed (*MachineKey*) from *web.config* (which the server trusts), enabling stealthier follow-up exploitation (Figure 1).

T1552: Unsecured Credentials

By accessing the deployed malicious endpoint, attackers can extract the cryptographic secrets needed to sign serialized payloads (Figure 2).

Indicators of compromise





NOTE
Manipulated Referer Header
CONTENT
Referer: /_layouts/SignOut.aspx

ACTION
Exploit Public-Facing Application
TACTIC
[ENT] TA0001 Initial Access
TECHNIQUE
[ENT] T1190 Exploit Public-Facing Application
DESCRIPTION
Attackers use an authentication bypass vulnerability in Microsoft SharePoint (on-prem) to send a specially crafted HTTP request with a manipulated Referer header to the ToolPane endpoint.

VULNERABILITY
CVE-2025-49706
DESCRIPTION
Improper authentication in Microsoft Office SharePoint allows an unauthorized attacker to perform spoofing over a network.

URL
VALUE
/_layouts/15/ToolPane.aspx?DisplayMode=Edit&a=/ToolPane.aspx

ACTION
Exploit Public-Facing Application
TACTIC
[ENT] TA0001 Initial Access
TECHNIQUE
[ENT] T1190 Exploit Public-Facing Application
DESCRIPTION
The same HTTP request also contains an exploit for a deserialization vulnerability that allows remote code execution.

VULNERABILITY
CVE-2025-49704
DESCRIPTION
Improper control of generation of code ("code injection") in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.

ACTION
PowerShell
TACTIC
[ENT] TA0002 Execution
TECHNIQUE
[ENT] T1059.001 PowerShell
DESCRIPTION
The deserialization exploit leads to execution of a powershell payload.

NOTE
Akamai / Unit 42 Variant 2
CONTENT
This attack path shows the post-exploitation behavior observed in the Akamai report. (Unit 42 published nearly identical intelligence that they called "Variation 2".)

ACTION
Web Shell
TACTIC
[ENT] TA0003 Persistence
TECHNIQUE
[ENT] T1505.003 Web Shell
DESCRIPTION
The attackers deploy an ASPX web shell that is capable of extracting cryptographic signing keys.

FILE
spinstall0.aspx

IPV4_ADDR
VALUE
107.191.58.76

IPV4_ADDR
VALUE
104.238.159.149

IPV4_ADDR
VALUE
96.9.125.147

DOMAIN_NAME
VALUE
dynastyjusticecollective.site

NOTE
Unit42 Variant 1
CONTENT
This attack path shows the post-exploitation behavior observed in the Unit 42 report labeled "Variation 1".

ACTION
Automated Collection
TACTIC
[ENT] TA0009 Collection
TECHNIQUE
[ENT] T1119 Automated Collection
DESCRIPTION
The payload iterates over the webroot recursively looking for web.config files and extracting their contents.

NOTE
Unit42 Variant 3
CONTENT
This attack path shows the post-exploitation behavior observed in the Unit 42 report labeled "Variation 3".

ACTION
Obfuscated Files or Information
TACTIC
[ENT] TA0005 Defense Evasion
TECHNIQUE
[ENT] T1027 Obfuscated Files or Information
DESCRIPTION
The Powershell payload is base64 encoded.

ACTION
Reflective Code Loading
TACTIC
[ENT] TA0005 Defense Evasion
TECHNIQUE
[ENT] T1620 Reflective Code Loading
DESCRIPTION
The web shell uses reflection to access the web configuration from memory.

ACTION
Unsecured Credentials
TACTIC
[ENT] TA0006 Credential Access
TECHNIQUE
[ENT] T1552 Unsecured Credentials
DESCRIPTION
The web shell extracts the MachineKey from memory.

ACTION
Exfiltration Over C2 Channel
TACTIC
[ENT] TA0010 Exfiltration
TECHNIQUE
[ENT] T1041 Exfiltration Over C2 Channel
DESCRIPTION
The attacker exfiltrates the MachineKey through the the web shell.

ACTION
Local Data Staging
TACTIC
[ENT] TA0009 Collection
TECHNIQUE
[ENT] T1074.001 Local Data Staging
DESCRIPTION
The contents of web.config files are staged in a new file called debug_dev.js.

FILE
\\PROGRA~1\\COMMON~1\\MICROS~1\\WEBSE~1\\16\\TEMPLATE\\LAYOUTS\\debug_dev.js

ACTION
Reflective Code Loading
TACTIC
[ENT] TA0005 Defense Evasion
TECHNIQUE
[ENT] T1620 Reflective Code Loading
DESCRIPTION
The web shell uses reflection to access the web configuration from memory.

FILE
\\PROGRA~1\\COMMON~1\\MICROS~1\\WEBSE~1\\16\\TEMPLATE\\LAYOUTS\\spinstall0.aspx

FILE
\\PROGRA~1\\COMMON~1\\MICROS~1\\WEBSE~1\\16\\TEMPLATE\\LAYOUTS\\spinstall0.aspx

ACTION
Unsecured Credentials
TACTIC
[ENT] TA0006 Credential Access
TECHNIQUE
[ENT] T1552 Unsecured Credentials
DESCRIPTION
The web shell extracts the MachineKey from memory.

ACTION
Exfiltration Over C2 Channel
TACTIC
[ENT] TA0010 Exfiltration
TECHNIQUE
[ENT] T1041 Exfiltration Over C2 Channel
DESCRIPTION
The attacker exfiltrates the MachineKey through the the web shell.

ACTION
Exfiltration Over C2 Channel
TACTIC
[ENT] TA0010 Exfiltration
TECHNIQUE
[ENT] T1041 Exfiltration Over C2 Channel
DESCRIPTION
The adversary exfiltrates the staged data over HTTP.
CONFIDENCE
Speculative

ACTION
ViewState Persistence
TACTIC
[ENT] TA0003 Persistence
DESCRIPTION
The attacker uses the stolen MachineKey to forge the ASP.NET VIEWSTATE, which allows code execution even after the CVEs are patched and the web shells are removed.

NOTE
Ysoserial
CONTENT
For example, ysoserial is an open source tool that forges ViewState cookies given a MachineKey.
<https://github.com/pwntester/ysoserial.net>

Using Attack Flow for Investigations

Overview

Findings

All

Included findings 4

- Unusual Volume of Network Activity Detect...
- Malicious PowerShell Process - Encoded ...
- Excessive Failed Logins
- 24 hour risk threshold exceeded for ...



Intermediate findings details 2

Search Show 10

Time	Description	Detection	Risk score	Annotations	Threat object
Today, 05:26	Excessive Failed Logins	Excessive Failed Logins	60	--	--
Yesterday, 18:30	Excessive Failed Logins	Excessive Failed Logins	60	--	--

Additional fields

- All entities: 10.11.36.2
- Annotation framework: cis20, nist, mitre_attack
- Annotations: T1030, Credential Access, Initial Access
- Application: ssh

Info

Owner: unassigned Status: New

Urgency: Informational Sensitivity: Unassigned

Disposition: Undetermined

ID: ES-00003

Type: INVESTIGATION

Time: Sep 17th, 2025 5:51 AM

Last updated: Sep 17th, 2025 5:51 AM

Reference ID: e46d0f23-3b9b-4d07-af80-7e031aa7ab1c

Investigation type: default

Description:

Notes 0

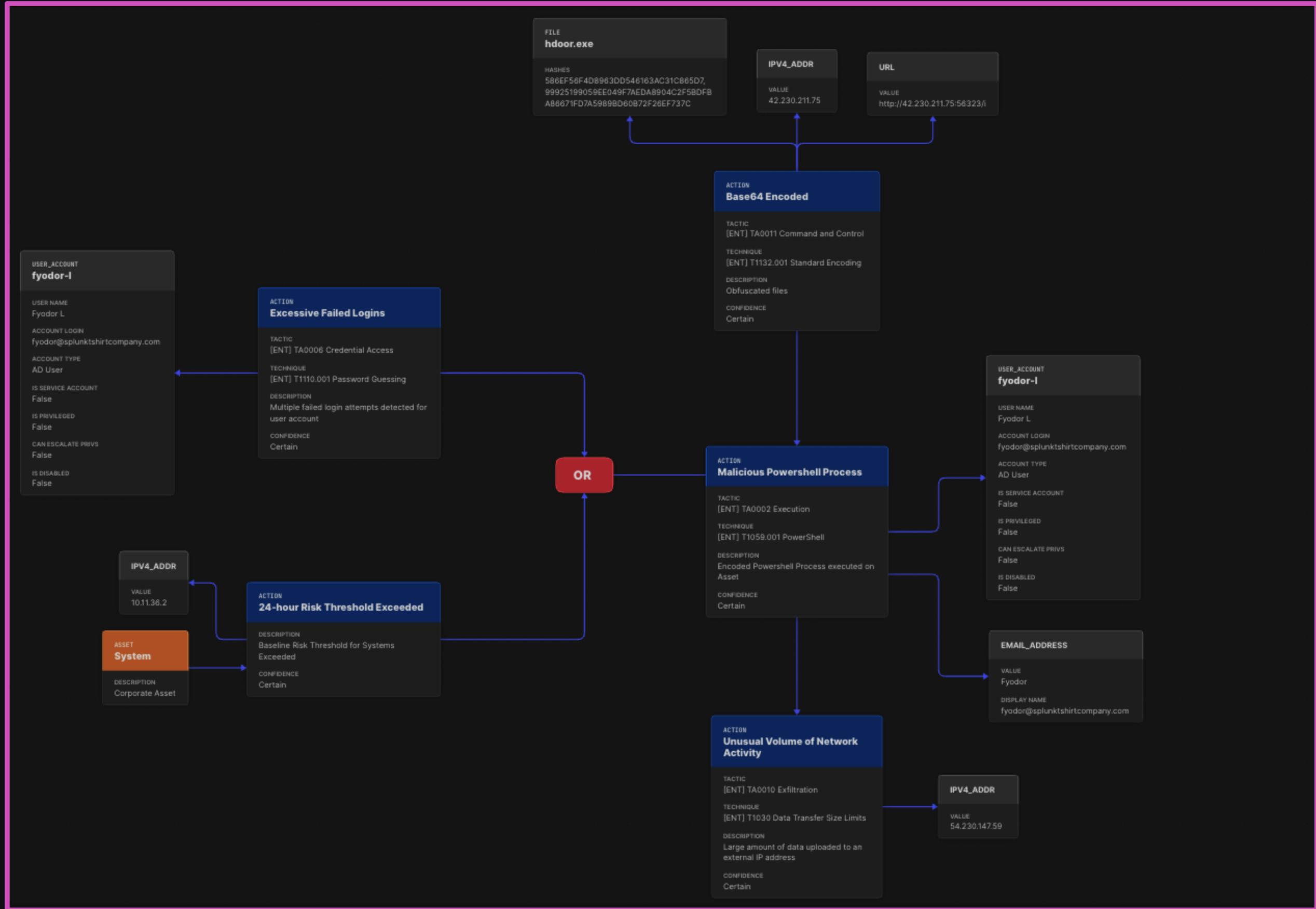
Enter title

Enter note

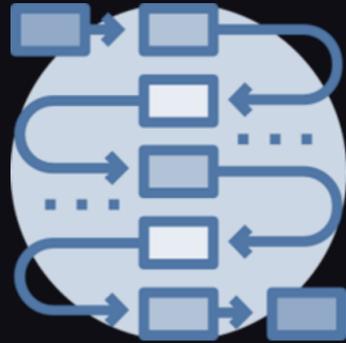
Save

Files 0

Drop your file here or upload file...
all file types supported



Components of Attack Flow



Attack Flow Builder Tool

- Web-based tool for creating, editing and presenting flows
 - Easily publish & share



Attack Flow Library

- A collection of example flows
- Used for learning about attacks and/or data mining



Machine-Readable Format

- Based on STIX 2.1
- Interoperability between vendors



Visualisation

- Tools for visualising flows for different audiences and purposes

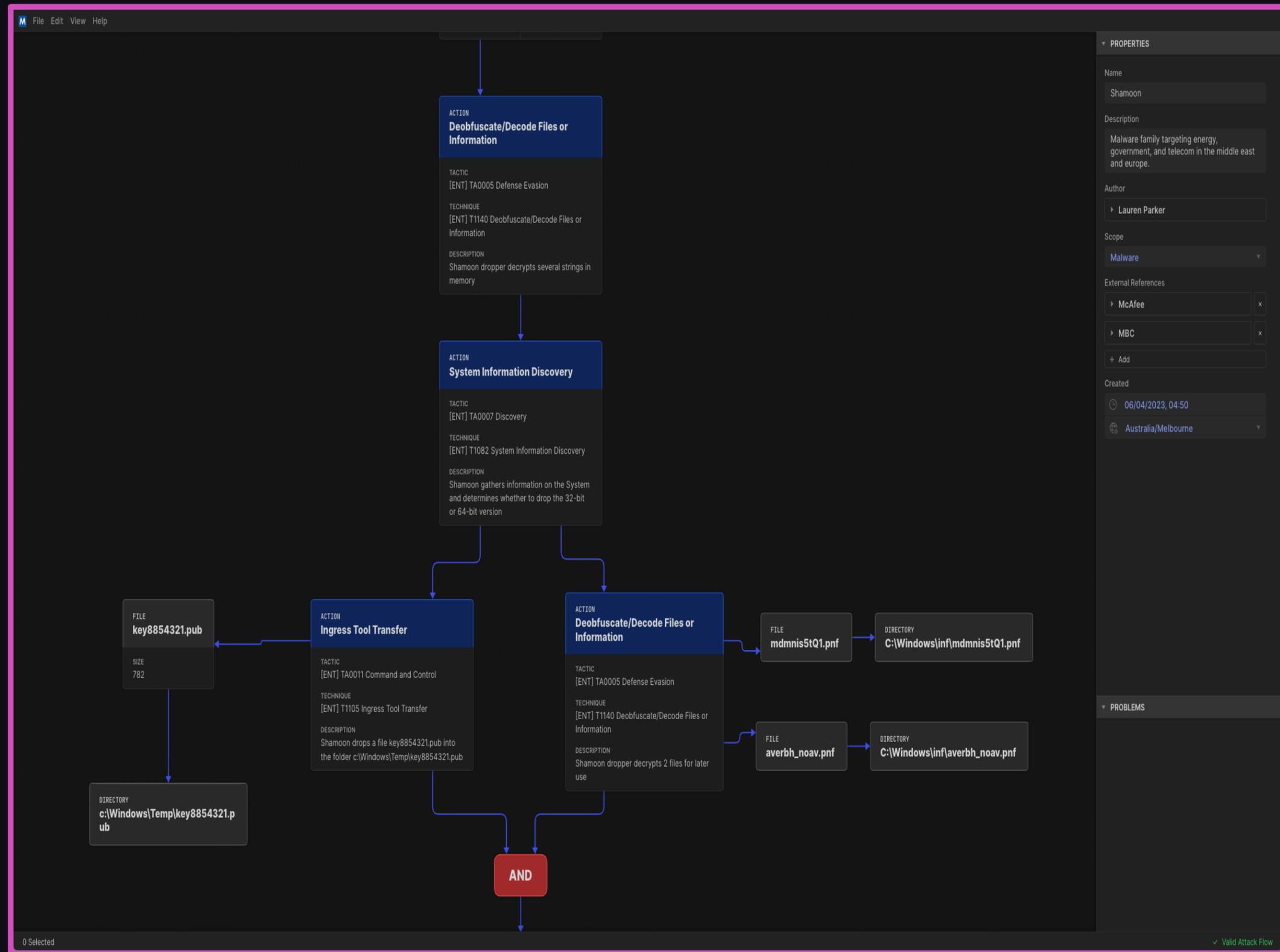


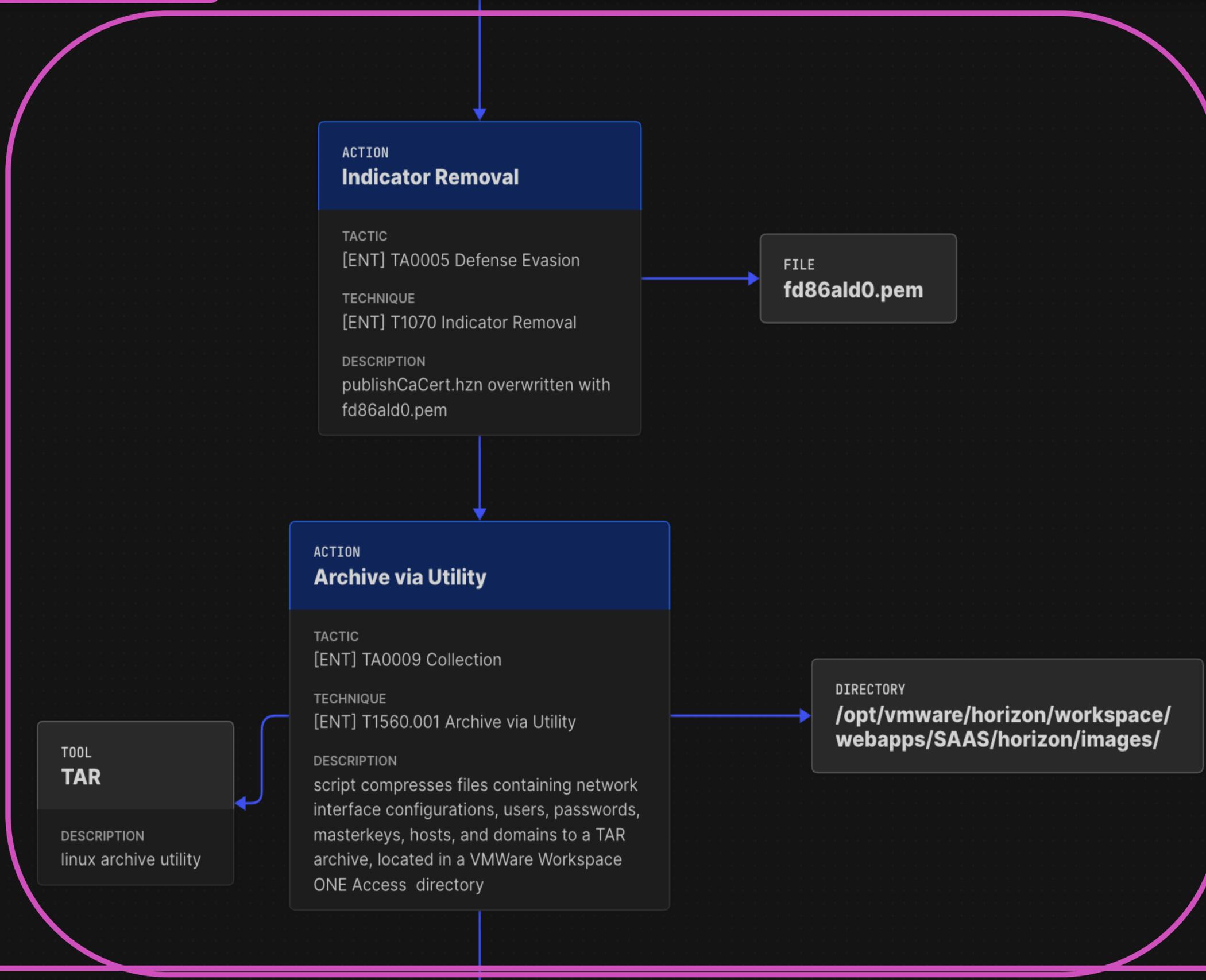
Documentation

- User-friendly learning curve
- Easy access to the builder & flow library

Component 1 - Attack Flow Builder Tool

- Open-source, web-based tool.
- Similar to Visio: create nodes (boxes) and connect with edges (lines).
- Create, edit, export and present flows.
- Private: flow data stays in the browser. CTID does not collect or share it.
- Can be hosted on-premise for additional privacy & assurance.





PROPERTIES

Name: CISA AA22-138B VMWare Workspace (Alt)

Description: Alternative method used to exploit VMWare Workspace ONE Access

Author: ▶ Lauren Parker

Scope: Incident

External References: ▶ CISA

PROBLEMS

Undo	⌘Z
Redo	⌘Y
Create	>
Select All	⌘A
Unselect All	Esc
Reset Zoom	⌘1
Zoom In	
Zoom Out	
✓ Animations	
✓ Shadows	

Attack Flow	>
Stix Object	>
Stix Observable	>
Dynamic Line	

Action
Asset
Condition
OR Operator
AND Operator

Attack Flow Block

Undo	⌘Z
Redo	⌘Y
Create	>
Select All	⌘A
Unselect All	Esc
Reset Zoom	⌘1
Zoom In	
Zoom Out	
✓ Animations	
✓ Shadows	

Attack Flow	>
Stix Object	>
Stix Observable	>
Dynamic Line	

Attack Pattern
Campaign
Course Of Action
Grouping
Identity
Indicator
Infrastructure
Intrusion Set
Location
Malware
Malware Analysis
Note
Observed Data
Opinion
Report
Threat Actor
Tool
Vulnerability
Marking Definition

STIX Domain Objects (SDO)

Undo	⌘Z
Redo	⌘Y
Create	>
Select All	⌘A
Unselect All	Esc
Reset Zoom	⌘1
Zoom In	
Zoom Out	
✓ Animations	
✓ Shadows	

Attack Flow	>
Stix Object	>
Stix Observable	>
Dynamic Line	

Artifact
Autonomous System
Directory
Domain Name
Email Address
Email Message
File
Ipv4 Addr
Ipv6 Addr
Mac Addr
Mutex
Network Traffic
Process
Software
Url
User Account
Windows Registry Key
X509 Certificate

STIX Cyber Observable (SCO)

Component 2 - Attack Flow Library

- A collection of example flows, based mostly on real-world CTI.
- Each example contains references to source material
- Open each example in Attack Flow Builder (.afb) or download as image (.png)

The screenshot shows the MITRE Attack Flow v3.0.0 documentation page. The page is titled "Example Flows" and is part of the "Docs" section. The MITRE logo and "Center for Threat Informed Defense" are visible in the top right corner. A search bar is located in the top left. The page content includes a navigation menu on the left with links for Overview, Introduction, Example Flows (highlighted), Builder, Training, Usage Guides, Visualization, Language, and Developers. The main content area features a "List of Examples" section with three entries: "Black Basta Ransomware", "CISA AA22-138B VMWare Workspace (Alt)", and "CISA AA22-138B VMWare Workspace (TA1)". Each entry includes the author's name, a description, and links to open the flow in the Attack Flow Builder or download it as an image (PNG) or Mermaid diagram. A "Light mode" toggle is visible in the top right of the content area.

ATTACK FLOW v3.0.0 MITRE Center for Threat Informed Defense

Search docs

Docs > Example Flows Light mode

Example Flows

The Attack Flow project includes a corpus of example flows that may be useful for learning about Attack Flow, studying high-profile breaches, or mining the data for statistical patterns. You can download the entire corpus from the [Attack Flow release page](#), or you can view individual flows on this page.

List of Examples

Black Basta Ransomware

Author: Lauren Parker

Description: Black Basta is a RaaS (Ransomware as a Service), written in C++, that has been in development since February 2022 and in active use since April 2022. Operators using Black Basta employ a double-extortion technique where they encrypt files on the target systems and demand payment for the decryption key while also threatening to leak the information if they are not paid.

Open: [Attack Flow Builder](#)

Download: [Attack Flow](#) | [STIX](#) | [GraphViz \(PNG\)](#) | [Mermaid](#)

CISA AA22-138B VMWare Workspace (Alt)

Author: Lauren Parker

Description: Alternative method used to exploit VMWare Workspace ONE Access

Open: [Attack Flow Builder](#)

Download: [Attack Flow](#) | [STIX](#) | [GraphViz \(PNG\)](#) | [Mermaid](#)

CISA AA22-138B VMWare Workspace (TA1)

Author: Lauren Parker

Description: Threat Actor 1 exploited VMWare Workspace ONE Access through various methods

Open: [Attack Flow Builder](#)

Download: [Attack Flow](#) | [STIX](#) | [GraphViz \(PNG\)](#) | [Mermaid](#)

Example Flows
List of Examples
Formats

Component 3 – Visualisation

- Extract data from an Attack Flow and generate insight by visualising it in new ways
- Automatically generate TTP tables or timeline views – a huge time saver.

ATTACK FLOW V3.0.0 MITRE | Center for Threat Informed Defense

Q Search docs

Overview
Introduction
Example Flows
Builder
Training
+ Usage Guides
Visualization
Language
Developers

Visualization

Attack Flow offers several tools for visualizing sequences of behaviors. The [Attack Flow Builder](#) is a great option, offers easy navigation of large flows, and exports to PNG format.

Visualization

- ATT&CK Navigator
- Tactic Table
- Matrix View
- Timeline View
- Treemap View



ATT&CK Navigator

Tactic Table

Matrix View

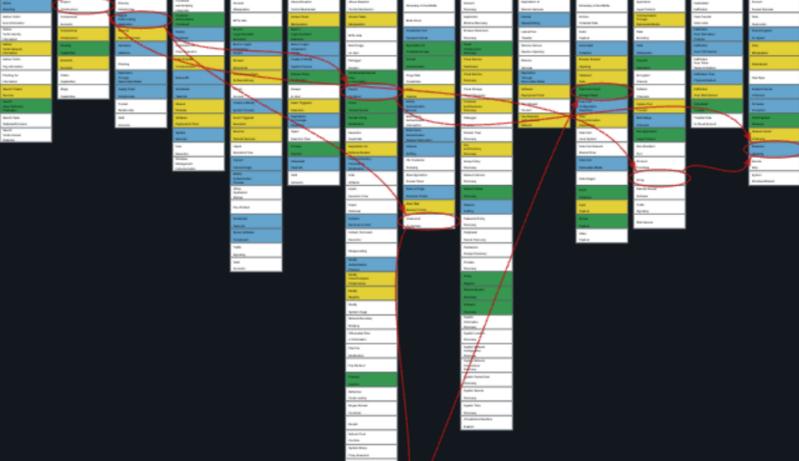
Timeline View

Treemap View

ATT&CK Navigator

With this visualization, you can visualize an Attack Flow drawn on top of an ATT&CK Navigator matrix. First, choose a Navigator base layer or supply your own. Then upload an Attack Flow. Finally, preview and download the resulting visualization.

[Try out the Navigator Visualization](#)



Visualisation



Attack Flow



STIX



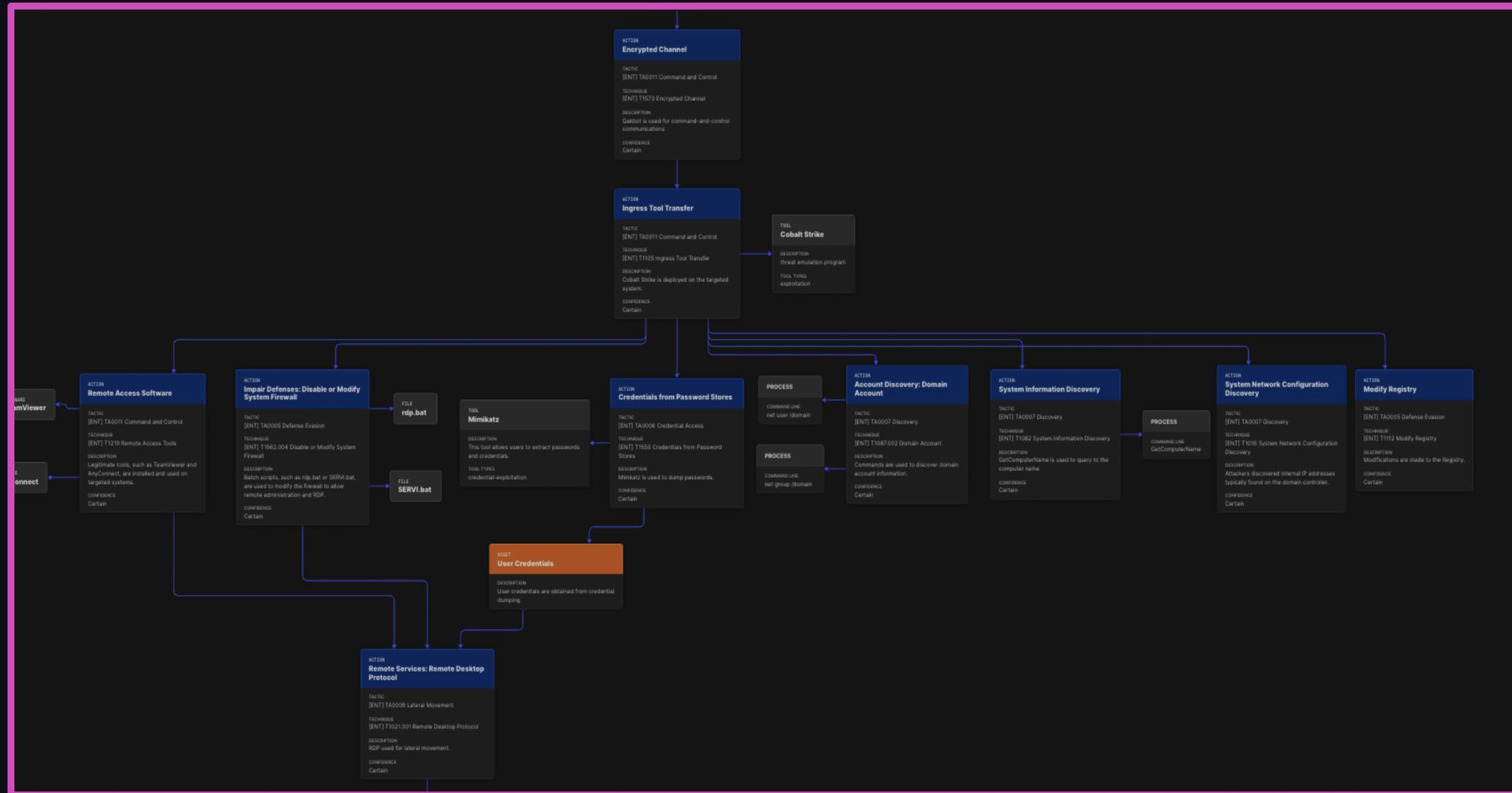
Portable Network Graphic



GraphViz



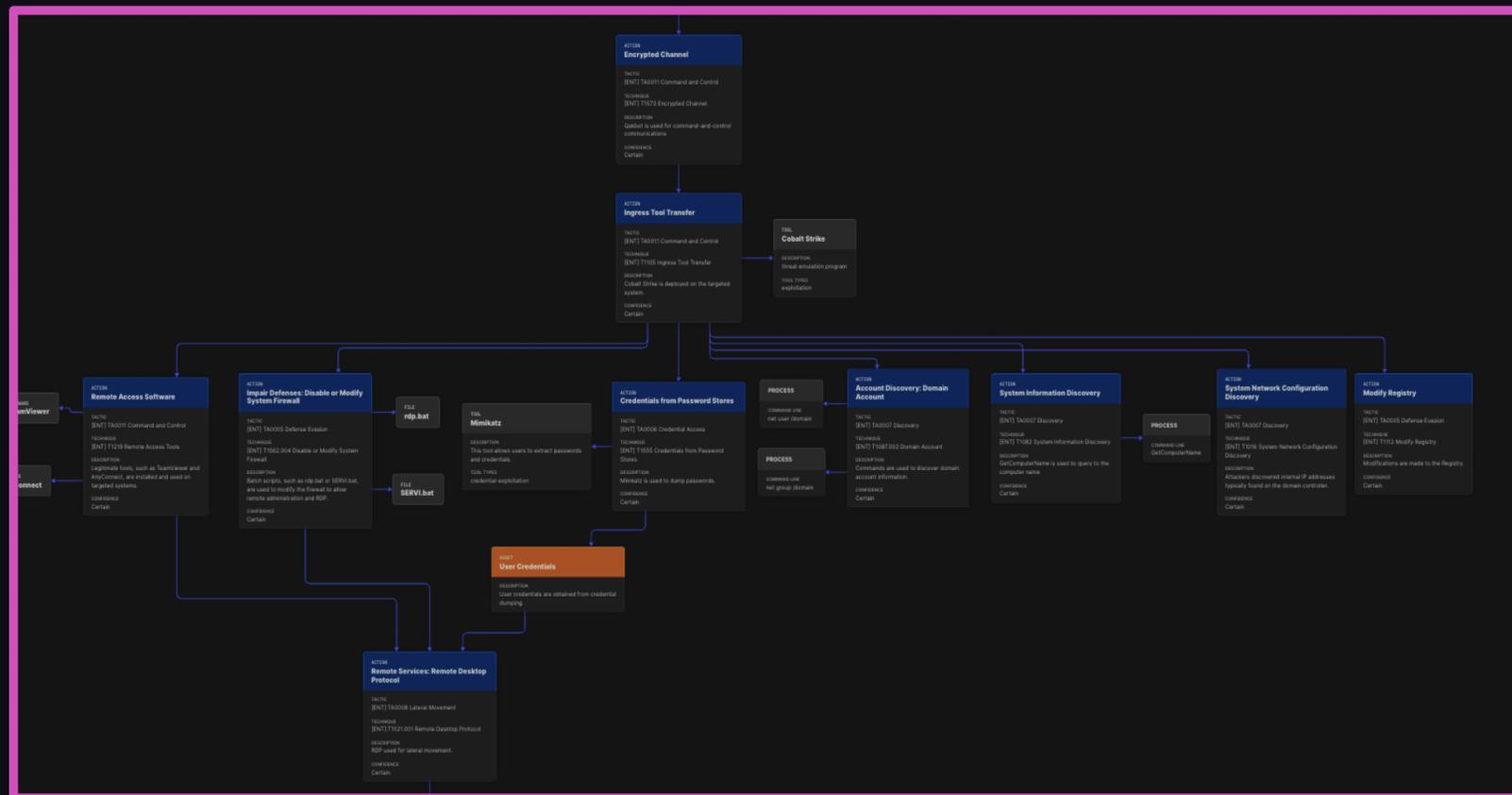
Mermaid.js



Visualisation

Save time through Automation

- Automate artifacts that are currently made by hand (or not at all)



Generate insights

- View data in new ways, or mashed up with other data sources
- Derive new insights

ATT&CK Navigator

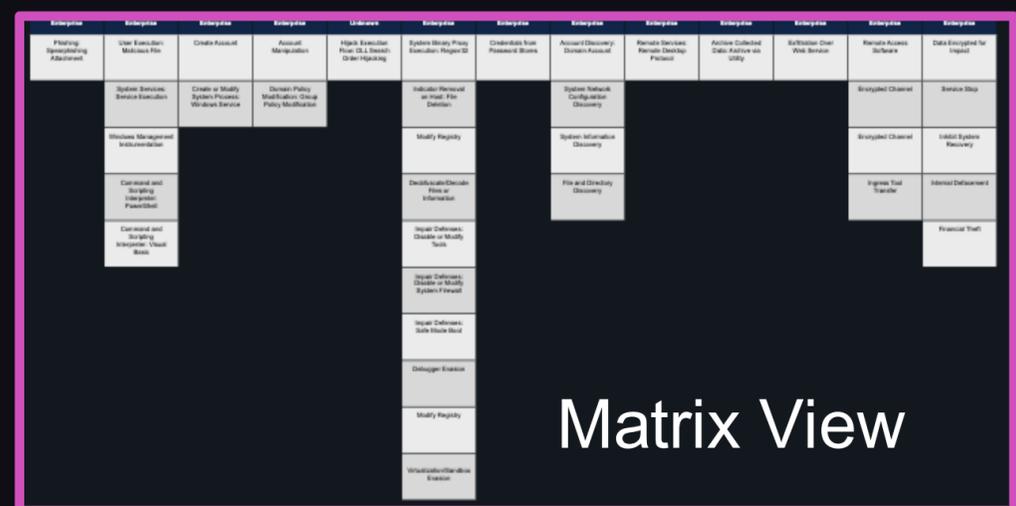
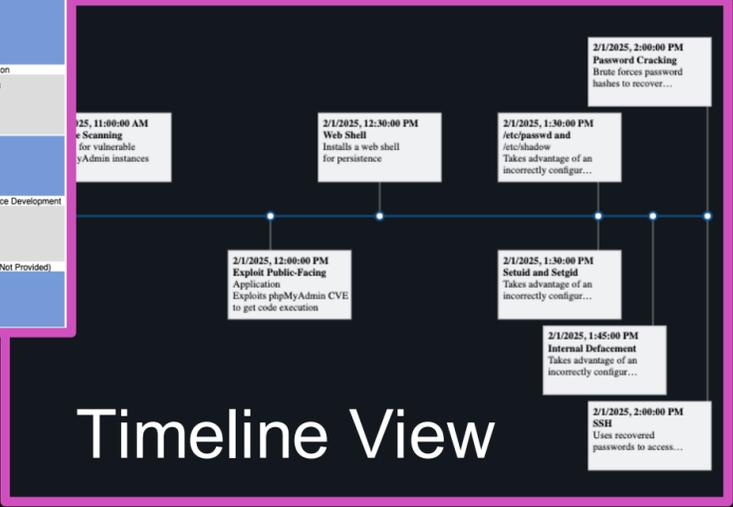
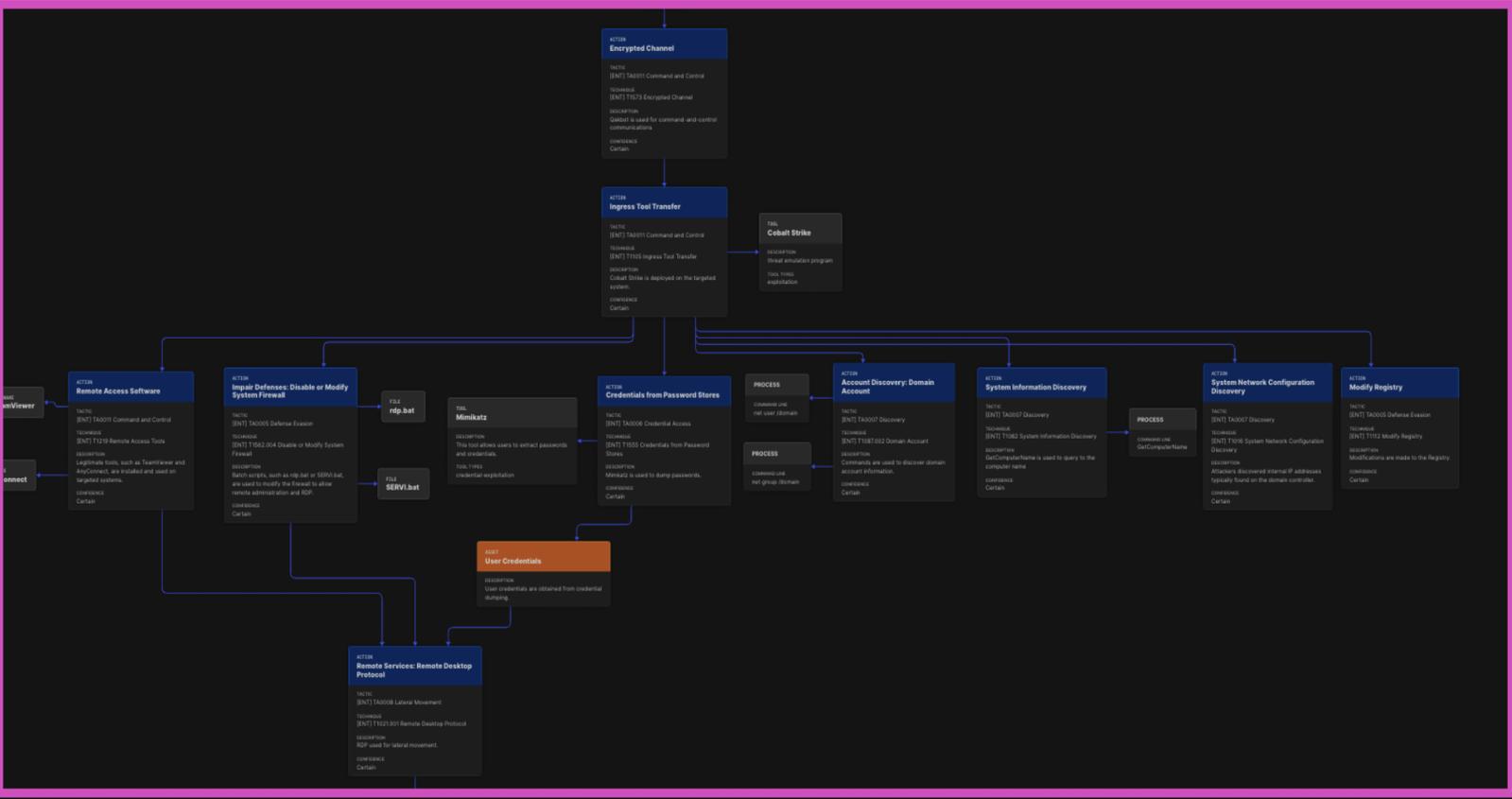


Table 1: TA0001 - Initial Access (Enterprise)

Technique Name	ATT&CK ID	Use
Phishing: Spearphishing Attachment	T1566.001	Victims receive spear phishing emails with malicious zip files attached.

Table 2: TA0002 - Execution (Enterprise)

Technique Name	ATT&CK ID	Use
User Execution: Malicious File	T1204.002	The zip files are extracted and usually contain a malicious document, such as a .doc, .pdf, or .xls.
System Services: Service Execution	T1569.002	Black Basta installs and uses PsExec to execute payloads on remote hosts.
Windows Management Instrumentation	T1047	Invoke-TotalExec is used to push out the ransomware binary.
Command and Scripting Interpreter: PowerShell	T1059.001	Within the malicious files, encoded PowerShell scripts are used to download additional malicious scripts.
Command and Scripting Interpreter: Visual Basic	T1059.005	The extracted files contain malicious macros.



Tactic Table

Treemap View

Timeline View

Matrix View

Component 4 – Documentation

- A complete guide to learning Attack Flow, starting from the ground up
- Links to builder tool and visualisations
- Usage guides for applying Attack Flow to specific job roles

ATTACK FLOW v3.0.0

MITRE | Center for Threat Informed Defense

Search docs

Docs > Overview

Light mode

Overview

Defenders think in lists. Attackers think in graphs. As long as this is true, attackers will win.

—John Lambert, [April 26, 2015](#)

Introduction

The Attack Flow project helps defenders move from tracking individual adversary behaviors to tracking the sequences of behaviors that adversaries employ to move towards their goals. By looking at combinations of behaviors, defenders learn the relationships between them: how some techniques set up other techniques, or how adversaries handles uncertainty and recover from failure. The project supports a wide variety of use cases: from blue team to red team, from manual analysis to autonomous response, and from front-line worker to the C-suite. Attack Flow provides a common language and toolset for describing complex, adversarial behavior.

Who is Attack Flow For?

This project is targeted at any cyber security professional seeking to understand how adversaries operate, the impact on their organization, and how to most effectively improve their defensive posture to address those threats. Threat intelligence analysts, security operations, incident response teams, red team members, and risk assessors are some of the groups that can benefit from Attack Flow. This specification facilitates sharing of threat intelligence, communicating about risks, modeling efficacy of security controls, and more. The project includes tools to visualize attacks for the benefit of low-level analysis as well as communicating high-level principles to management.

Use Cases

Attack Flow is designed to support many different use cases.

Threat Intelligence

CTI analysts can use Attack Flow to create highly detailed, behavior-based threat intelligence products. The language is machine-readable to provide for interoperability across organizations and commercial tools. Users can track adversary behavior at the incident level, campaign level, or threat actor level. Instead of focusing on indicators of compromise (IOCs), which are notoriously inexpensive for the adversary to change, Attack

Impact



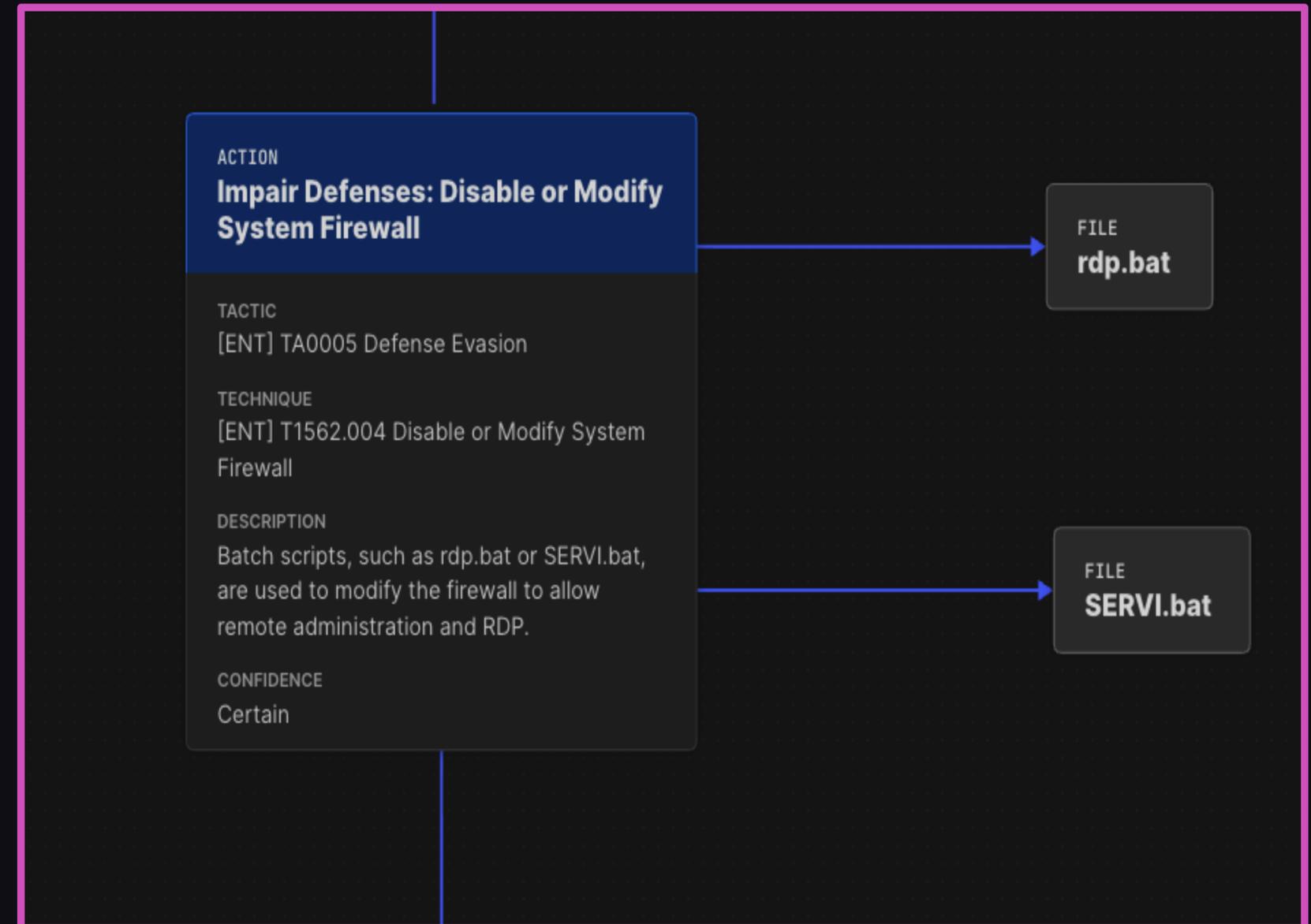
Help defenders and leaders understand how adversaries operate and compose atomic techniques into attacks to better understand defensive posture

Attack Flow

Why it matters?

Less Ambiguous

- Prose reports contain significant ambiguity, especially around the order of events, dependencies and confidence levels.
- Attack Flow clarifies how an adversary works through a sequence of behaviours to reach their desired impact.
- Models how adversaries handle failure and recovery.



Increase Automation

- Machine readable format is compatible with STIX; import & export IOCs easily
- Visualisation tools automatically create artifacts such as TTP tables or attack timelines
- Open source: coders can build custom tooling

```
1 {
2   "type": "bundle",
3   "id": "bundle--bd17b78b-2ffd-45db-a4b0-d1104b95c2db",
4   "spec_version": "2.1",
5   "created": "2025-07-30T19:47:12.605Z",
6   "modified": "2025-07-30T19:47:12.605Z",
7   "objects": [
8     {
9       "type": "extension-definition",
10      "id": "extension-definition--fb9c968a-745b-4ade-9b25-c324172197f4",
11      "spec_version": "2.1",
12      "created": "2022-08-02T19:34:35.143Z",
13      "modified": "2022-08-02T19:34:35.143Z",
14      "name": "Attack Flow",
15      "description": "Extends STIX 2.1 with features to create Attack Flows.",
16      "created_by_ref": "identity--fb9c968a-745b-4ade-9b25-c324172197f4",
17      "schema": "https://center-for-threat-informed-defense.github.io/attack-flow/stix/attack-flow-schema-2.0.0.json",
18      "version": "2.0.0",
19      "extension_types": [
20        "new-sdo"
21      ],
22      "external_references": [
23        {
24          "source_name": "Documentation",
25          "description": "Documentation for Attack Flow",
26          "url": "https://center-for-threat-informed-defense.github.io/attack-flow"
27        },
28        {
29          "source_name": "GitHub",
30          "description": "Source code repository for Attack Flow",
31          "url": "https://github.com/center-for-threat-informed-defense/attack-flow"
32        }
33      ]
34    },
35    {
36      "type": "identity",
37      "id": "identity--fb9c968a-745b-4ade-9b25-c324172197f4",
38      "spec_version": "2.1",
39      "created": "2022-08-02T19:34:35.143Z",
40      "modified": "2022-08-02T19:34:35.143Z",
41      "created_by_ref": "identity--fb9c968a-745b-4ade-9b25-c324172197f4",
42      "name": "MITRE Center for Threat-Informed Defense",
43      "identity_class": "organization"
44    },
45    {
46      "type": "attack-flow",
47      "id": "attack-flow--042142d6-2080-4c1d-8ef2-bad02c39db3b",
48      "spec_version": "2.1",
49      "created": "2024-06-19T15:45:49.090Z",
50      "modified": "2025-07-30T19:47:12.606Z",
51      "extensions": {
52        "extension-definition--fb9c968a-745b-4ade-9b25-c324172197f4": {
53          "extension_type": "new-sdo"
54        }
55      },
56      "created_by_ref": "identity--0b55fa9f-cd34-442f-a59e-8dae3ff9c0a7",
57      "start_refs": [
58        "attack-action--a3679838-b02f-4c2b-a0b6-d3450ca2e1dd"
59      ]
60    }
61  ]
62 }
```

Line 1, Column 1 — 1375 Lines

Who is it for?

- **Cyber Threat Intelligence Analysts**
 - Use Attack Flow to augment CTI reporting.
 - Automatically generate generating artifacts, example – export STIX IOCs, generate timeline view, create TTP table, etc.
- **Incident Response**
 - Use Attack Flow to document incident investigations as they develop.
 - Confidence and notes feature to highlight what's known vs. unknown and where to focus next.
- **Red Team**
 - Plan Red Team scenarios based on known threat actors; start at high level and work down to procedure level.
 - Record execution notes and use the flow to debrief Blue Team.

Resources

- Learn more about MITRE –
 - <https://www.mitre.org/focus-areas/cybersecurity>
- MITRE ATT&CK® Framework –
 - <https://attack.mitre.org>
- Know more about MITRE CTID –
 - <https://ctid.mitre.org>
- Project Website -
 - <https://center-for-threat-informed-defense.github.io/attack-flow/>

Next Steps

- Visit the Project Website –
 - <https://center-for-threat-informed-defense.github.io/attack-flow/>
 - Shortlink -> ctid.io/flow
- Open an existing flow and learn about a published breach
- Find an open-source CTI report and try build your own flow for it
 - <https://github.com/center-for-threat-informed-defense/attack-flow>

Questions?

Thank You