

Attack Flow Training: 1 – Introduction to Attack Flow

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?

Together, we are changing the rules of the game



+ MITRE

Membership is:

- ✓ Highly-sophisticated
- ✓ Global & cross-sector
- ✓ Non-governmental
- ✓ Committed to collaborative R&D in the public interest

IT TAKES A VILLAGE



MITRE | Center for Threat
Informed Defense



<https://ctid.mitre.org>

Attack Flow – Motivation



PROBLEM

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



SOLUTION

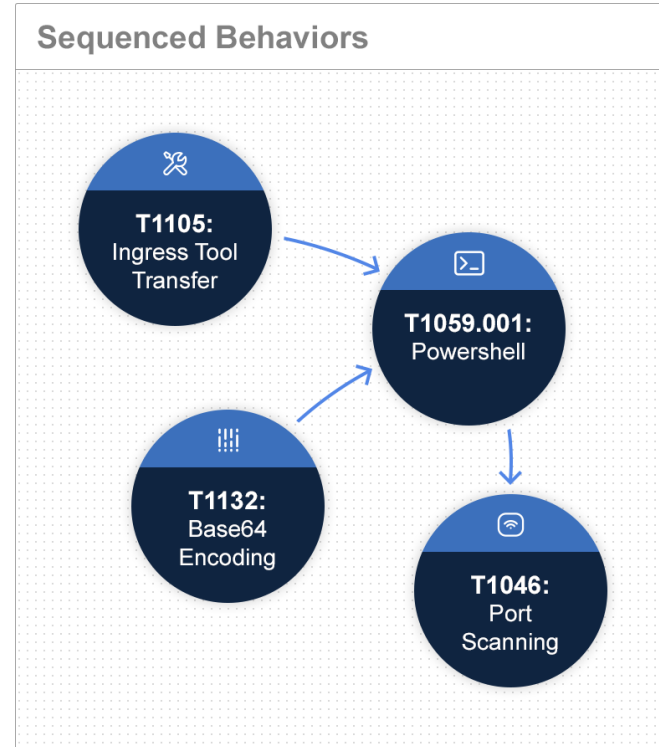
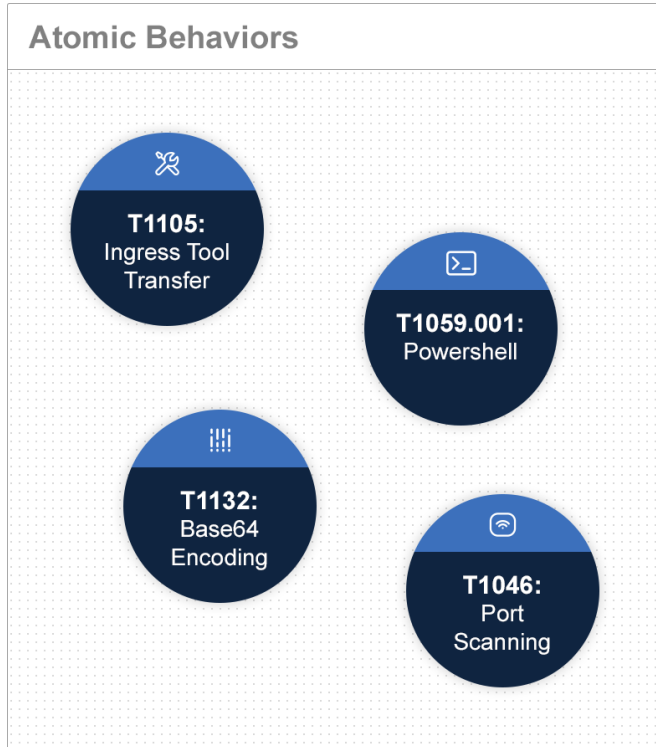
Create a language, and associated tooling, to describe flows of ATT&CK techniques and combine those flows into patterns of behavior.



IMPACT

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


Describing Adversary Behavior




Tesla Incident: Atomic Behaviors

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**, Contributor
Posted in Zero Day on February 20, 2018 | Topic: Security




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 documents the discovery of an unprotected Kubernetes console belonging to automaker Tesla.

The Kubernetes console is used to automate the deployment,




RELATED

Best Java bootcamps: Where to learn Java (and why you should)

The 9 best cloud storage services: Cost, free storage, and features compared

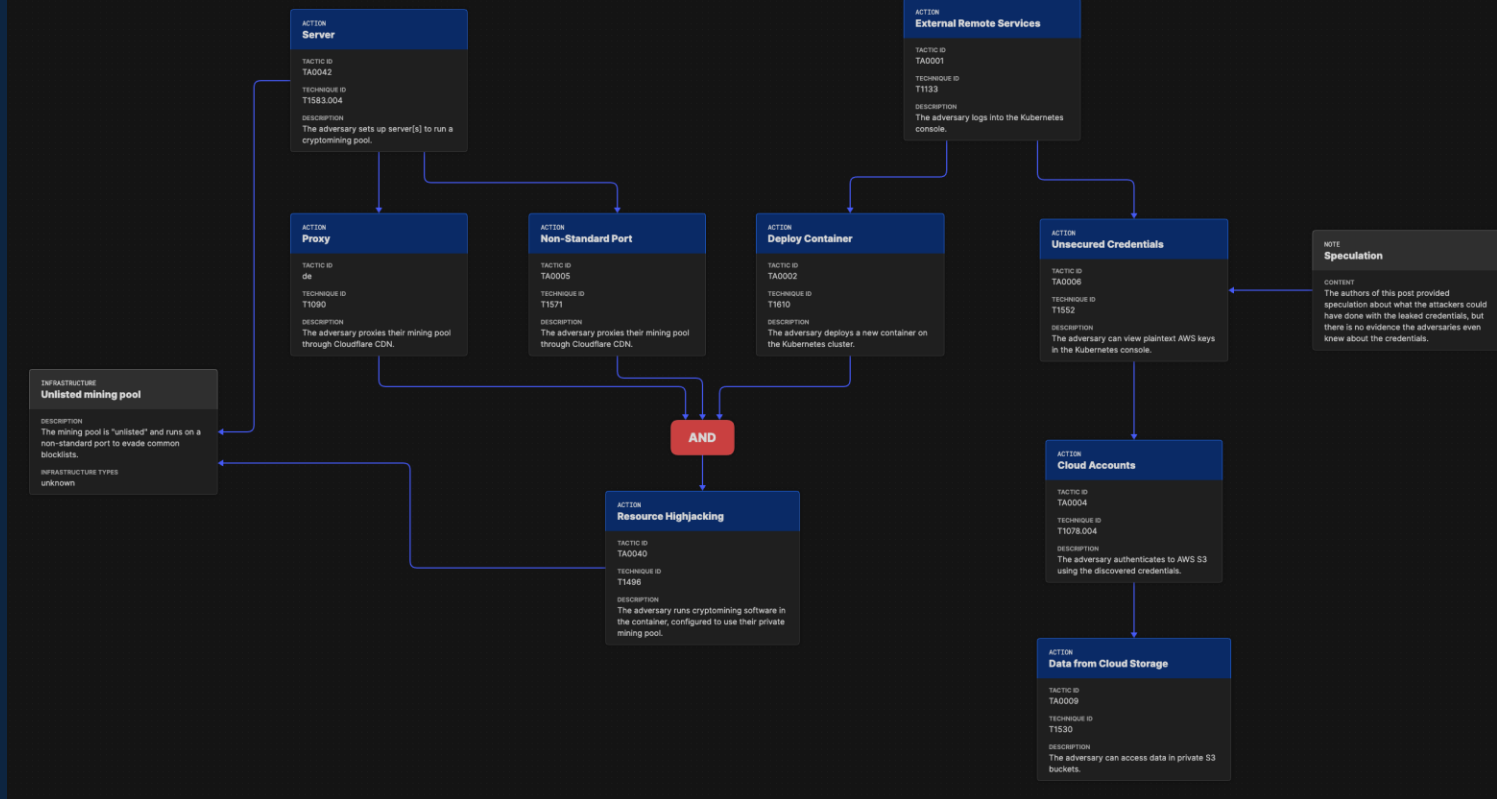
The best smart speakers: Should you go with Alexa, Siri, or Google Assistant?





| 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 (5) | Drive-by Compromise | Command and Scripting Interpreter (10) | Account Manipulation (10) | Abuse Elevation Control Mechanism (10) | Abuse Elevation Control Mechanism (10) | Adversary-In-the-Middle (10) |
| Gather Victim Host Information (10) | Compromise Accounts (5) | Exploit Public-Facing Application | Container Administration Command | BITS Jobs | Access Token Manipulation (10) | Access Token Manipulation (10) | Brute Force (10) |
| Gather Victim Identity Information (10) | Compromise Infrastructure (5) | External Remote Services | Deploy Container | Boot or Logon Autostart Execution (10) | Boot or Logon Autostart Execution (10) | Boot or Logon Autostart Execution (10) | Credentials from Password Stores (10) |
| Gather Victim Network Information (10) | Develop Capabilities (5) | Hardware Additions | Exploitation for Client Execution | Boot or Logon Initialization Scripts (10) | Boot or Logon Initialization Scripts (10) | Boot or Logon Initialization Scripts (10) | Exploitation for Credential Access |
| Gather Victim Org Information (10) | Establish Accounts (5) | Phishing (10) | Inter-Process Communication (10) | Browser Extensions | Create or Modify System Process (10) | Deobfuscate/Decode Files or Information | Forced Authentication |
| Phishing for Information (10) | Obtain Capabilities (5) | Replication Through Removable Media | Native API | Compromise Client Native API (1100) | Domain Policy Modification (10) | Deploy Container | Forge Web Credentials (10) |
| Search Closed Sources (10) | Stage Capabilities (5) | Supply Chain Compromise (10) | Scheduled Task/Job (10) | Create Account (10) | Escape to Host | Direct Volume Access | Input Capture (10) |
| Search Open Technical Databases (10) | | Trusted Relationship | Shared Modules | Create or Modify System Process (10) | Event Triggered Execution (10) | Domain Policy Modification (10) | Modify Authentication Process (10) |
| Search Open Websites/Domains (10) | | Valid Accounts (10) | Software Deployment Tools | Event Triggered Execution (10) | Exploitation for Privilege Escalation | Execution Guardrails (10) | Multi-Factor Authentication Interception |
| Search Victim-Owned Websites | | | System Services (10) | External Remote Services | Hijack Execution Flow (10) | Exploitation for Defense Evasion | Multi-Factor Authentication Request Generation |
| | | | User Execution (10) | Hijack Execution Flow (10) | Process Injection (10) | File and Directory Permissions Modification (10) | Network Sniffing |
| | | | Windows Management Instrumentation | Implant Internal Image | Scheduled Task/Job (10) | Hide Artifacts (10) | OS Credential Dumping (10) |
| | | | | Modify Authentication Process (10) | Valid Accounts (10) | Hijack Execution Flow (10) | Steal Application Access Token |
| | | | | Office Application Startup (10) | | Indicator Removal on Host (10) | Steal or Forge Kerberos Tickets (10) |
| | | | | Pre-OS Boot (10) | | Indirect Command Execution | Steal Web Session Cookie |
| | | | | Scheduled Task/Job (10) | | Masquerading (10) | Unsecured Credentials (10) |
| | | | | Server Software Component (10) | | Modify Authentication Process (10) | |
| | | | | Traffic Signaling (10) | | Modify Cloud Compute Infrastructure (10) | |
| | | | | Valid Accounts (10) | | | |

Tesla Incident: Sequenced Behaviors



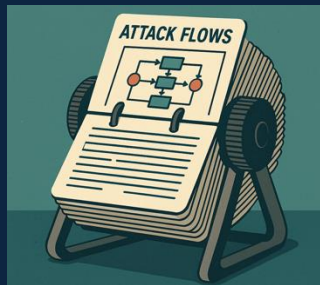
Attack Flow – What It Is

What's Included?



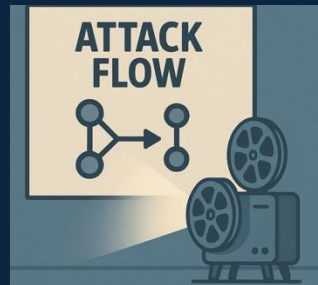
Attack Flow Builder

Web-based tool for creating, editing, and presenting flows.



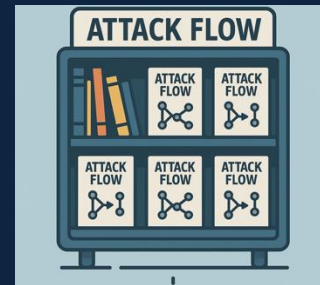
Flow Library

A collection of 34 example flows, useful for learning about Attack Flow, learning about breaches, and data mining.



Visualization

Tools for visualizing flows for different audiences and purposes.



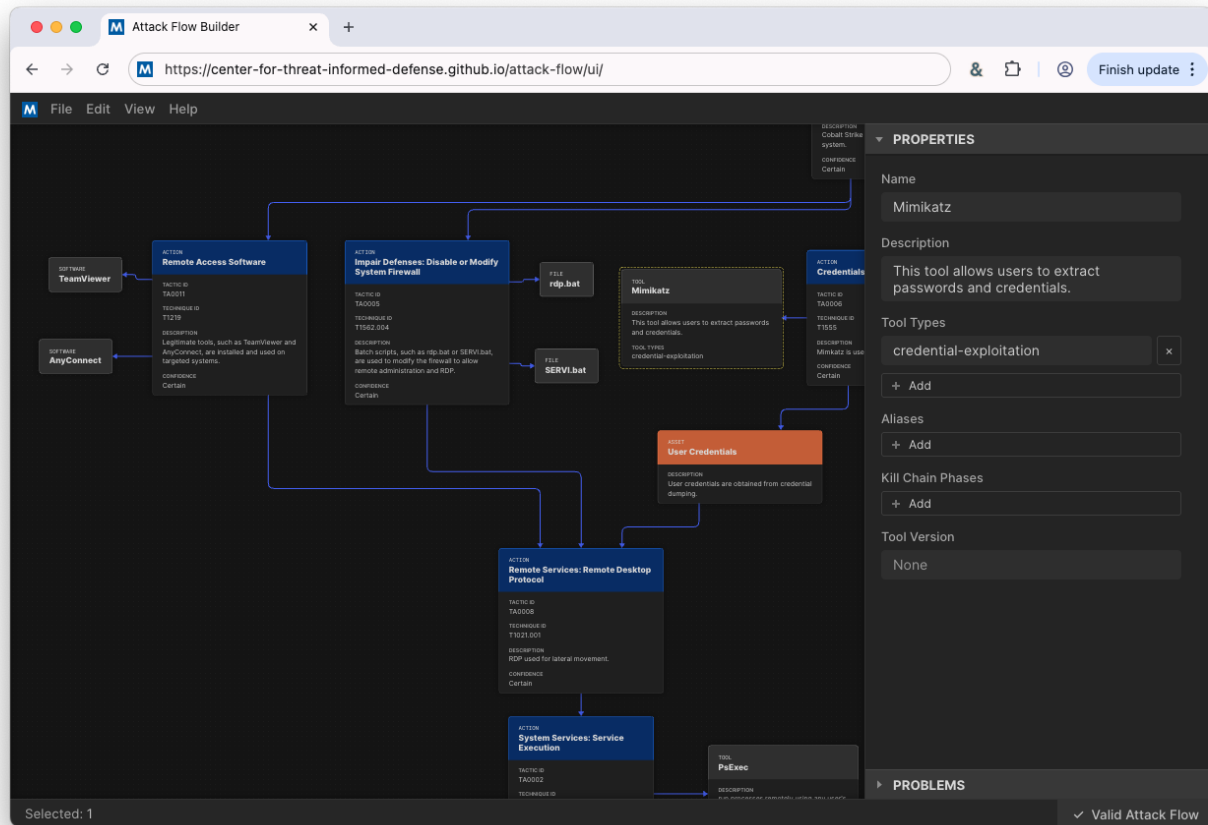
Documentation

User-friendly introduction to flow, easy access to the library and tools.

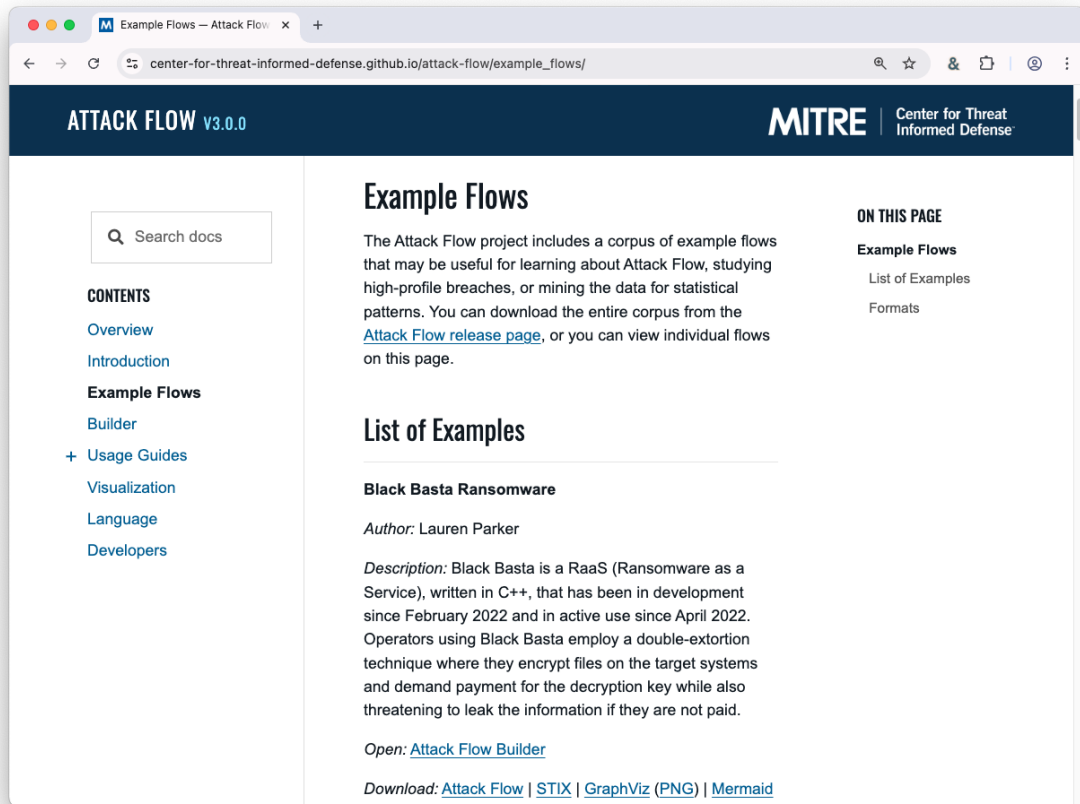


Attack Flow Builder

- Web-based tool for creating, editing, and presenting flows.
- Totally private: your flow data stays in the browser; we do not collect it or share it.



Flow Library



- A collection of 39 example flows, based mostly on real-world CTI.
- Each example contains references to source material.
- Open each example in Attack Flow Builder or download as image.

Visualization

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

The screenshot shows the MITRE ATT&CK Navigator v3.0.0 web application. The browser address bar shows the URL: center-for-threat-informed-defense.github.io/attack-flow/visualization/. The page has a dark blue header with the MITRE logo and the text "Center for Threat Informed Defense".

ATTACK FLOW v3.0.0

MITRE | Center for Threat Informed Defense

CONTENTS

- Overview
- Introduction
- Example Flows
- Builder
- + Usage Guides
- Visualization**
- Language
- Developers

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](#)

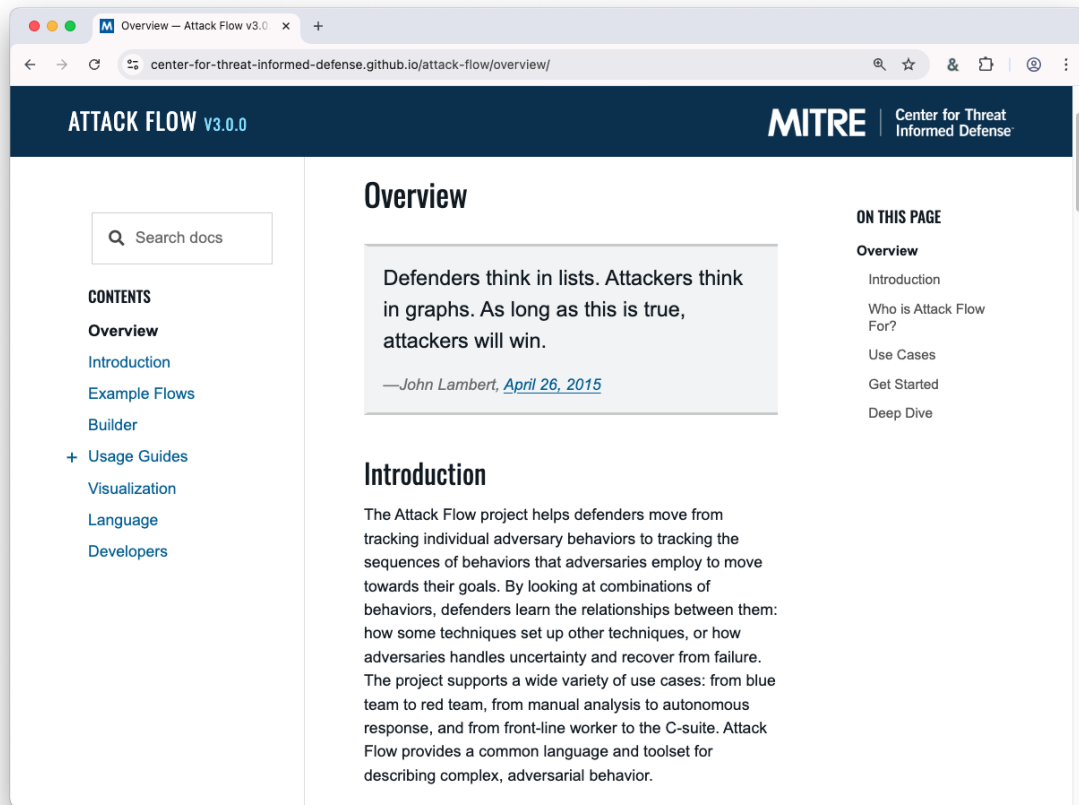
ON THIS PAGE

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

The main content area displays a "Tactic Table" which is a large matrix of MITRE ATT&CK tactics and techniques. Red lines and circles are overlaid on the matrix, indicating a specific attack flow path through various tactics and techniques.

Tactic Table

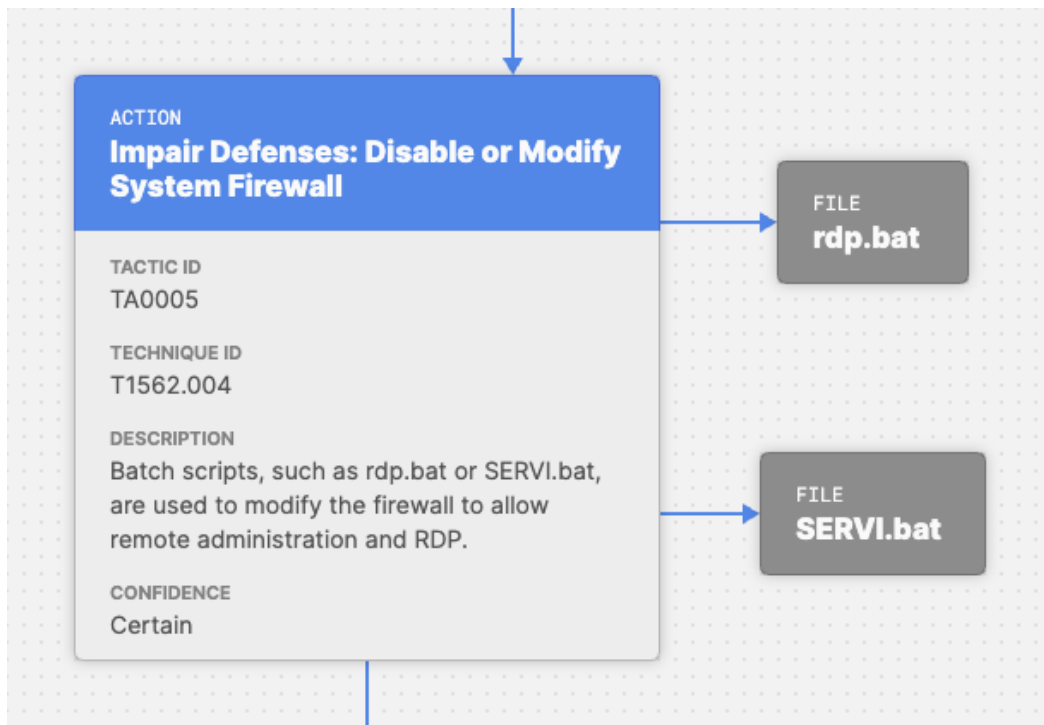
Documentation



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

Attack Flow – Why It Matters

Less Ambiguous



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

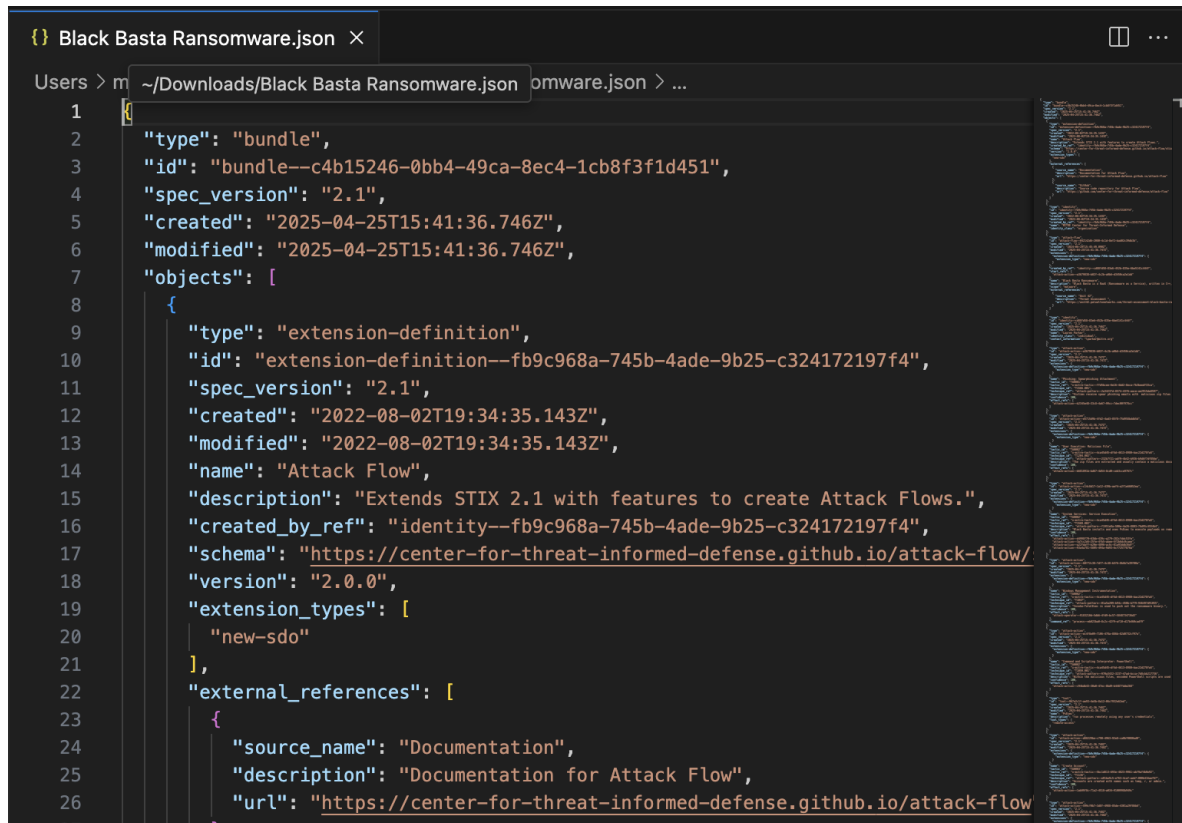
Visualize & Present

- Visualize attack paths and chokepoints.
- High quality presentations for a variety of audiences, including execs.
- Combine with other data to generate insights.

| Reconnaissance | Resource Development | Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access |
|------------------------------------|---------------------------------------|-------------------------------------|------------------------------------|-----------------------------------|--------------------------------------|------------------------------------|---|
| Phishing for Information | Acquire Accounts | Exploit Public-Facing Application | Software Deployment Tools | Valid Accounts | Valid Accounts | Valid Accounts | Enumerated Credentials |
| Active Scanning | Acquire Infrastructure | Valid Accounts | Command and Scripting Interpreter | Server Software Components | Abuse Elevation Controls Mechanism | Modify System Image | Live Binary in the Memory |
| Gather Victim Host Information | Compromise Accounts | Supply Chain Compromise | Inter-Process Communication | Create or Modify System Processes | Exploitation for Privilege Elevation | Abuse Elevation Controls Mechanism | Exploitation for Credential Access |
| Gather Victim Identity Information | Compromise Development Infrastructure | Developer Compromise | Windows Management Instrumentation | Create or Modify Pre-OS Boot | Exploitation for System Process | OS Credential Dumping | OS Credential Dumping |
| Gather Victim Network Information | Develop Capabilities | External Remote Services | Exploitation for Remote Execution | Hijack Execution Flow | Escape to Host | Indicators Removal | Steal Application Access Token |
| Gather Victim Origin Information | Establish Accounts | Phishing | Stealth Method Task Job | External Remote Services | Hijack Execution Flow | Subvert Trust Controls | Steal or Forge Kerberos Tickets |
| Search Coded Sources | Obtain Capabilities | Replication Through Removable Media | System Services | Modify Authentication Process | Schedule Task Job | System Binary Modification | Modify Authentication Process |
| Search Open Technical Databases | Stage Capabilities | Trusted Relationship | User Execution | Create Account | Domain or Tenant Policy Modification | Pre-OS Boot | Brute Force |
| Search Victim-Owned Websites | | Hardware Additions | Container Installation on many | Implement Intermittent | Process Injection | Hijack Execution Flow | Network Sniffing |
| Search Open Websites/Domains | | Content Injection | Deploy Container | NTS Jobs | Account Manipulation | Network Boundary Bypassing | Force Authentication |
| | | | Services Execution | Browser Extensions | Boot or Logon Initialization Scripts | Modify Authentication Process | Multi-Web Session Cookie |
| | | | Native API | Schedule Task Job | Event Triggered Execution | Impair Defenses | Multi-Factory Authentication Interception |
| | | | Cloud Administration Command | Off-C Application Startup | Access Token Manipulation | Debugger Evasion | Credentials from Password Store |
| | | | Shared | Account | | Pilot File | Forge Web |

Increase Automation

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



```
{
  "type": "bundle",
  "id": "bundle--c4b15246-0bb4-49ca-8ec4-1cb8f3fd451",
  "spec_version": "2.1",
  "created": "2025-04-25T15:41:36.746Z",
  "modified": "2025-04-25T15:41:36.746Z",
  "objects": [
    {
      "type": "extension-definition",
      "id": "extension-definition--fb9c968a-745b-4ade-9b25-c324172197f4",
      "spec_version": "2.1",
      "created": "2022-08-02T19:34:35.143Z",
      "modified": "2022-08-02T19:34:35.143Z",
      "name": "Attack Flow",
      "description": "Extends STIX 2.1 with features to create Attack Flows.",
      "created_by_ref": "identity--fb9c968a-745b-4ade-9b25-c324172197f4",
      "schema": "https://center-for-threat-informed-defense.github.io/attack-flow/",
      "version": "2.0.0",
      "extension_types": [
        "new-sdo"
      ],
      "external_references": [
        {
          "source_name": "Documentation",
          "description": "Documentation for Attack Flow",
          "url": "https://center-for-threat-informed-defense.github.io/attack-flow/"
        }
      ]
    }
  ]
}
```

Who is it for?

- **Cyber Threat Intelligence Analysts**

- Use Attack Flow to augment CTI reporting.
- Automatically generate generating artifacts, e.g. 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.

Who is using Attack Flow?

- Global community from US to EU to APAC.
- Multinational corporations and small business.
- Threat modelers, red teamers, CTI analysts, defenders.

Dave Johnson · 1st
Threat Intelligence Advisor @Feedly | Former FBI Analyst | Entrepren...
2mo · Edited · 🌐

I've been working on a secret ATT&CK Flow visualization tool 🤖


Why? Because it's winter in Wisconsin. ❄️

What does it do? It generates a graph of attack procedures in a threat intelligence report automatically, so you get the gist of detailed reports much faster.

It will also generate STIX bundles so you can do adversary emulation in tools like MITRE Caldera. Or, you can export into an image file to use in a custom report or presentation.

Drop a comment down below if you're interested! 🍌

#ThreatIntelligence #AdversaryEmulation #ATTACKFlow
#CyberSecurity



You can see the links, you can see the nodes, you can see the flow!

You and 421 others · 112 comments · 19 reposts

Like · Comment · Repost · Send

Dewank Pant · 1st
Security@Amazon (Alexa AI Security Research) | Lea...
(edited) 2mo · 🌐

Dave Johnson This is great! would love to collaborate on this. Some thoughts: these attack flow details could also be linked to an exploit crafting agent to generate new attack variants, speeding up security testing. This would also be valuable for prompt testing tools (like Garak and Pyrit), as jailbreak research papers come out every other day, this way we could feed in new papers and generate multiple attack variants to expand the test sets!

David Greenwood · 1st
I build products that make threat intelligence analysts go; "Wow! That's wh...
2mo · 🌐

txt2stix now supports automated Attack Flow extraction for MITRE ATT&CK references in reports.

I've update the last part of my blog post (linked in the post below) with some examples.

dogesec
1,765 followers
2mo · Edited · 🌐

For a long time, I, like many of you, have been tagging detection content with ATT&CK Techniques.

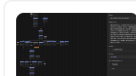
Sometimes, ashamedly, I tout full detection coverage for a particular threat. I show off the ATT&CK Navigator highlighting how all the detections cover the ATT&CK Techniques an intel team has discovered an adversary to use

The reality is, although this captures a lot of information, and is often better-than-nothing, it still lacks a key component – time (or flow!) of techniques.

Many people incorrectly read the ATT&CK Matrix as a flow. They assume the flow of an attack moves from left to right. This is incorrect in many instances where an attacker jumps backwards and forwards in their attempts to achieve an objective.

The point is this; the ATT&CK Matrix alone does not provide enough to describe how an adversary might work and that's where Attack Flows come in.

<https://lnkd.in/ezaPN4rB>



Beyond the ATT&CK Matrix: How to Build Dynamic Attack Flows with STIX
dogesec.com

Gert-Jan Bruggink · 1st
Founder & CEO, Venation | Proven Systems for Smarter Decisions.
Visit my website
2mo · Edited · 🌐

I've been successfully modeling threat scenarios for over 7 years. Here's how I recently updated my 'system' with Attack Flow:

I believe that cybersecurity needs a support function that helps understand variables (threats) that drive risk + support explicit decision making on what to do about it.

To do this right, you need a system.

Most teams understand WHY you need to do this. Some even have figured out HOW. Today, I'll show you WHAT you can do right now to integrate this in your daily workflow using Attack Flow.

Copy it into your internal procedures and create your own!

Let's make this week count!

Gert-Jan

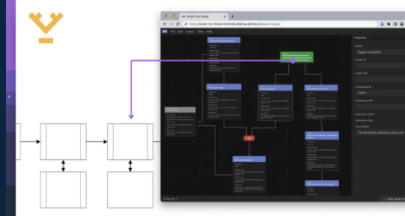
If you want systems directly in your mailbox, join our newsletter for the complete ones:

GO here: <https://lnkd.in/eWwxc5bQ>

Found my content useful?

Share it with your network & follow [Gert-Jan Bruggink](#) and [Venation](#) for more.

#CyberSecurity #RiskManagement #ThreatModeling #ThreatScenarios



End of Section 1