Attack Flow – Beyond Atomic Behaviors

Desiree Beck, Gabriel Bassett, Ryusuke Masuoka
30 June 2022
Who Are We?

Desiree Beck
Principal Cybersecurity Engineer
MITRE
dbeck@mitre.org

Gabriel Bassett
Lead Data Scientist and Co-author
Verizon DBIR
gabriel.bassett@verizon.com

Ryusuke Masuoka
Research Principal
Fujitsu System Integration Labs
masuoka.ryusuke@fujitsu.com

© 2022 MITRE Engenuity. Approved for public release. Document Number #CT0048
The Center for Threat-Informed Defense conducts collaborative R&D projects that improve cyber defense at scale.

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

© 2022 MITRE Engenuity. Approved for public release. Document Number #CT0048
Outline

• Problem
  • What’s the problem?
  • What’s an attack flow?

• Solution
  • Attack flow data format

• Impact
  • How do attack flows help?
  • Attack flow corpus
Problem
What’s the Problem?

• Defenders track adversary behaviors individually, but adversaries use *sequences* of techniques
  
• False positives harder to identify
• Incidents harder to understand
• Defensive planning is less effective
• Cyber assessments are less useful
What’s the Problem?

- Defenders track adversary behaviors individually, but adversaries use *sequences* of techniques

Sequences of techniques create *relationships*
What’s an Attack Flow?

An attack flow is a machine-readable representation of a sequence of actions and assets, plus knowledge properties.

© 2022 MITRE Engenuity. Approved for public release. Document Number #CT0048
How Do Attack Flows Help?

- Communication
- Intelligence exchange
- Operations
- Defensive planning
- Assessments
Solution
Learn by example
Schemas

- **JSON Schema**

  ```json
  object (8)
  
  schema: https://json-schema.org/draft/2020-12/schema
  id: https://mitre-engenuity.com/schema/attack-flow/2021-10-13-draft.json
  title: Attack Flow
  description: This schema describes the Attack Flow JSON format.
  type: object
  
  properties (6)
  
  flow (4)
  
  description: An Attack Flow Meta object
  type: object
  
  properties (6)
  
  type (3)
  
  description: Indicate that this is an Attack Flow.
  type: string
  
  enum [1]
  
  @: attack-flow
  
  id (3)
  
  description: The identifier for this Attack Flow. MUST be unique within this document. TODO: Ideally is unique among Attack Flows produced by a particular organization.
  
  type: string
  format: uri
  
  name (2)
  
  description: The name of the Attack Flow.
  type: string
  ```

- **RDF (Graph) Schema**
Short Interlude: RDF
What is RDF?

- RDF = Resource Description Framework
- URI = Unique Resource Identifier

RDF takes 3 URIs and turns them into a source node, relationship edge, and target node.
Ok, back to the example...
Start with data

• IR Report
  Incident 12345
  * Mail logs show User A receives phishing email and opens attached macro-enabled word document on Host B
  * Proxy and host logs detect Host B beaconing to known C2, downloading the ransomware, and running it

• Red Team Report
  Engagement 56789
  * Phished User A to run macro-enabled office document on Host B
  * Installed simulated ransomware through shell embedded in document on Host B

© 2022 MITRE Engenuity. Approved for public release. Document Number #CT0048
Structuring Data
Storage – JSON-SCHEMA
Storage – JSON-LD (Linked Data)
So what's it look like?
Attack Flow Data Format
Three C's: Causality, Context, Complexity
Attack Flow Data Format - Causality
Attack Flow Data Format - Context
Attack Flow Data Format – Complexity
Attack Flow Data Format – Complexity
Analysis
### Analysis

**SPARQL Query & Update**

```sparql
PREFIX ats: <https://vz-risk.github.io/faw/attack-flow/>
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX DISTINCT :asset

WHERE {
  ?asset rdf:type ats:asset.
}
```

---

**Filter query results**

<table>
<thead>
<tr>
<th>Asset</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>asset1</td>
<td>Phishing</td>
</tr>
<tr>
<td>asset2</td>
<td>Malware</td>
</tr>
<tr>
<td>asset3</td>
<td>Ransomware</td>
</tr>
<tr>
<td>asset4</td>
<td>DoS</td>
</tr>
<tr>
<td>asset5</td>
<td>Exploitation</td>
</tr>
</tbody>
</table>

---

**Analysis**

- `<https://github.com/center-for-threat-informed-defense/attack_to_veris>`
- `atk:T1566`
- `atk:T1486`
- `atk:T1586`
- `atk:T1003.001 - T1003.005, T1555.002`
- `atk:T1219`
- `atk:T1014`
- `atk:T1595`
- `atk:T1190`

© 2022 MITRE Engenuity. Approved for public release. Document Number #CT0048
Impact
Better Communication

- Document incident lessons learned
- Visualize IR/Threat Intel/Red Team data
  - Aggregate like nodes & actions
  - Filter tangential properties to simplify
- Explain defensive posture to executives
Better Communication

- Explain defensive posture to executives
Better Intelligence Exchange

• Attack flow sightings can be shared machine-to-machine
• Graph pattern communication
Better Operations

- **Attack flow queries**
  - Determining paths to/from an adversary technique difficult to mitigate
  - Query datasets for strategic insights (what happens the most → most important for me to mitigate)
Better Defensive Planning

• Understand attack surfaces (attack graph generation)
• Analyze risk
• Aggregate attack flows
• Build and communicate non-atomic detections
  • Hinges on data in records being properties that are connected to ground-truth actions and assets
• Identify cyberthreat choke points
  • Enables disruption of the adversary’s attack model

© 2022 MITRE Engenuity. Approved for public release. Document Number #CT0048
Better Assessments

• Build Realistic Adversary Emulation Scenarios
  • Data driven red teaming
  • Subgraphs are key and are strung together:
    *If we succeed in action X on an asset, then we will attempt action Y from that asset*

• Pen Testing
• Breach and Attack Simulation
  • Logic operator is key
  • Pair attack flow with planner & choose from available options
• Operation Cobalt Kitty
• Conti Ransomware Incident
• “From Zero to Domain Admin”
• “Mac Malware Steals Cryptocurrency”
• “Right to Left Override”
• Tesla’s Kubernetes Breach

Please Contribute

Become an early adopter!

• Prototype capabilities
• Create structured reports – submit attack flows to corpus
• Provide feedback as GitHub issues

• Project Summary
  • https://ctid.mitre-engenuity.org/our-work/attack-flow
• “Attack Flow – Beyond Atomic Indicators”
  • https://medium.com/mitre-engenuity/attack-flow-beyond-atomic-behaviors-c646675cc793
• GitHub
  • https://github.com/center-for-threat-informed-defense/attack-flow
  • https://github.com/vz-risk/flow

© 2022 MITRE Engenuity. Approved for public release. Document Number #CT0048
Questions?