VECTRA®
SECURITY THAT THINKS

Using Rapid Threat Model Prototyping

For Testing Threat Detection Efficacy

Tom D'Aquino

Oct. 30th, 2023

About Me

- Director of Security Validation at Vectra AI
  - tomdaq@vectra.ai
- Creator of ./HAVOC
  - https://havoc.sh
  - https://github.com/havocsh
  - https://havoccommunity.slack.com/
- Strongly opinionated voice On LinkedIn
  - https://linkedin.com/in/tomdaquino

Objectives of Security Validation

- What questions are we trying to answer?
  - Can we detect advanced attacker TTPs?
  - Will detections end up where they're supposed to (SIEM)?
  - Will the associated entities be prioritized appropriately?
  - Do we have enough information to respond appropriately?
  - What response actions are necessary to contain a breach by an advanced attacker?

Setting the Stage

- Emphasis is on defending against advanced adversaries
  - Assume preventative controls will be bypassed
    - Zero-day exploits
    - Evasive payloads, traffic profiles and infrastructure
  - Assume opportunistic / adaptive attack techniques
- Post-compromise detection efficacy is top priority
  - Assessing advanced detection capabilities i.e., not signature-based solutions
    - AI-based and behavioral-based detection capabilities
    - Traps and tripwires

Purple Team (non)Planning

Common Approach

- Breach headline instigates reactionary measures
  - Gather TTPs
  - Conduct a tabletop exercise, identify priorities
  - Conduct testing of prioritized TTPs
    - Tests are limited to known exploits and known-bad artifacts
      - Mostly oriented around preventative controls

Purple Team (non)Planning

Common Approach

- Breach headline instigates reactionary measures
  - Gather TTPs
  - Conduct a tabletop exercise, identify priorities
  - Conduct testing of prioritized TTPs
    - Tests are limited to known exploits and known-bad artifacts
      - Mostly oriented around preventative controls
- Reasons Tom is wagging his finger
  - Tom is not a fan of reactionary approaches
  - Scope of TTPs is too narrow
  - Didn’t we agree that advanced adversaries will bypass preventative controls?
  - Didn’t we agree that advanced adversaries are opportunistic?

And One More Thing

- Attack “samples” and “replays” are not adequate for testing AI-based capabilities

And One More Thing

- Attack “samples” and “replays” are not adequate for testing AI-based capabilities
  - Example of a sample: A short session (2 or 3 minutes) that mimics the requests and responses of a well-known C2 traffic profile
    - Fine for signature-based solutions but won’t meet the criteria of a real C2 session from the perspective of an AI-based solution

And One More Thing

- Attack “samples” and “replays” are not adequate for testing AI-based capabilities
  - Example of a sample: A short session (2 or 3 minutes) that mimics the requests and responses of a well-known C2 traffic profile
    - Fine for signature-based solutions but won’t meet the criteria of a real C2 session from the perspective of an AI-based solution
  - Example of a replay: Replaying a PCAP of a previously recorded session executing an Smbexec attack

And One More Thing

- Attack “samples” and “replays” are not adequate for testing AI-based capabilities
  - Example of a sample: A short session (2 or 3 minutes) that mimics the requests and responses of a well-known C2 traffic profile
    - Fine for signature-based solutions but won’t meet the criteria of a real C2 session from the perspective of an AI-based solution
  - Example of a replay: Replaying a PCAP of a previously recorded session executing an Smbexec attack
    - Previously recorded traffic is not applicable to the production environment being monitored by the AI-based solution
    - Replaying previously recorded traffic is constrained to only a few hosts - lacks interaction with the production environment being monitored by the AI-based solution

Testing Methodology Overview

Rapid Threat Model Prototyping (RTMP) with MITRE ATT&CK

1

Model the System

- Summarize the environment
- Compose a high-level architecture
- Identify sources: Attack origin
- Identify sinks: Target of value

2

Analyze Threats

- Create an attack tree that is relevant to the tech being tested
- Map MITRE ATT&CK Tactics to attack tree stages
- Identify applicable MITRE ATT&CK Techniques

3

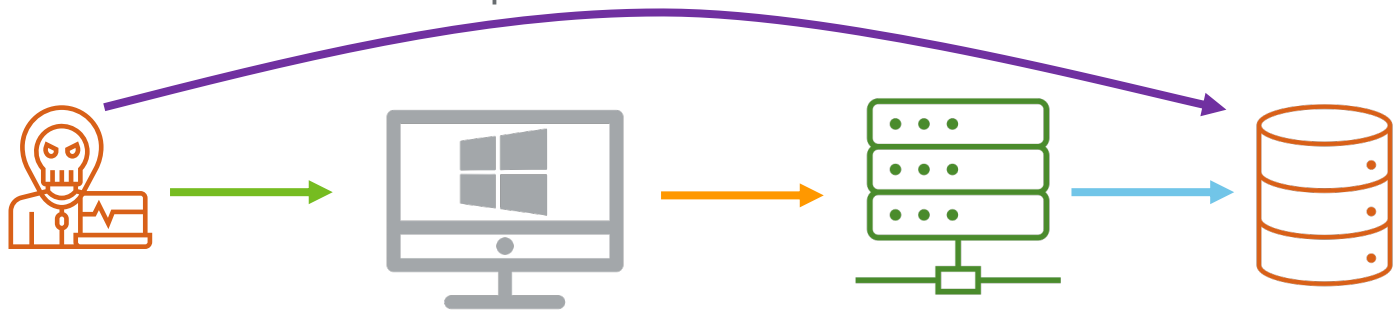
Analyze Mitigations

- Identify opportunities for detecting attacker's techniques
- Focus on mitigations that are relevant to the tech being tested

4

Validate

- Emulate TTPs
- Confirm traffic flows
- Review detections
- Confirm event pipeline
- Review downstream alerts, dashboards, and reports



https://resources.infosecinstitute.com/topics/management-compliance-auditing/rapid-threat-model-prototyping-introduction-and-overview/

Rapid Threat Model Prototyping (RTMP) with MITRE ATT&CK

Model the System

Example Environment Summary

Architecture

- Enterprise IT environment
  - Multi-campus network
    - Workstation VLAN spans across campus offices (Tier 2)
  - Three Data centers
    - Server VLANs (Tier 0 and Tier 1) span across three data centers
      - Standard AD Domain, file/print services
      - Finance and HR applications
      - Customer data analytics
      - Engineering development infrastructure
      - IT infrastructure and applications
- Production services environment (not in scope)
  - Publicly accessible customer services and infrastructure

Example Environment Summary

Accessibility

- Tiered administration model (workstations, general servers, authentication servers)
  - Tier 0: Authentication servers (domain controllers, ADFS, etc.), IT infrastructure & applications
  - Tier 1: All other servers
  - Tier 2: Workstations
- Administrative ports (RDP, WinRM) are restricted to bastion hosts for each tier
- SMB is denied between workstations and denied from workstations to most servers except where required
- Access to each tier is restricted to users assigned to the tier
  - Tier 0: ‘username-t0’ + MFA
  - Tier 1: ‘username-t1’ + MFA
  - Tier 2: Standard username – MFA required when accessing bastion hosts
- Engineering users in Tier 2 have access to production services environment via special bastion hosts

https://blog.palantir.com/restricting-smb-based-lateral-movement-in-a-windows-environment-ed033b888721

Example Environment Summary

North/South Traffic Policies

- Inbound traffic:
  - Inbound DNS: None
  - Inbound HTTP/HTTPS: None
  - Other inbound protocols: None
- Outbound traffic:
  - Outbound DNS: Restricted to DNS servers
  - Outbound HTTP/HTTPS: Permitted without restriction
  - Other outbound protocols: By exception only

- Remote users access data center applications via Zscaler ZPA

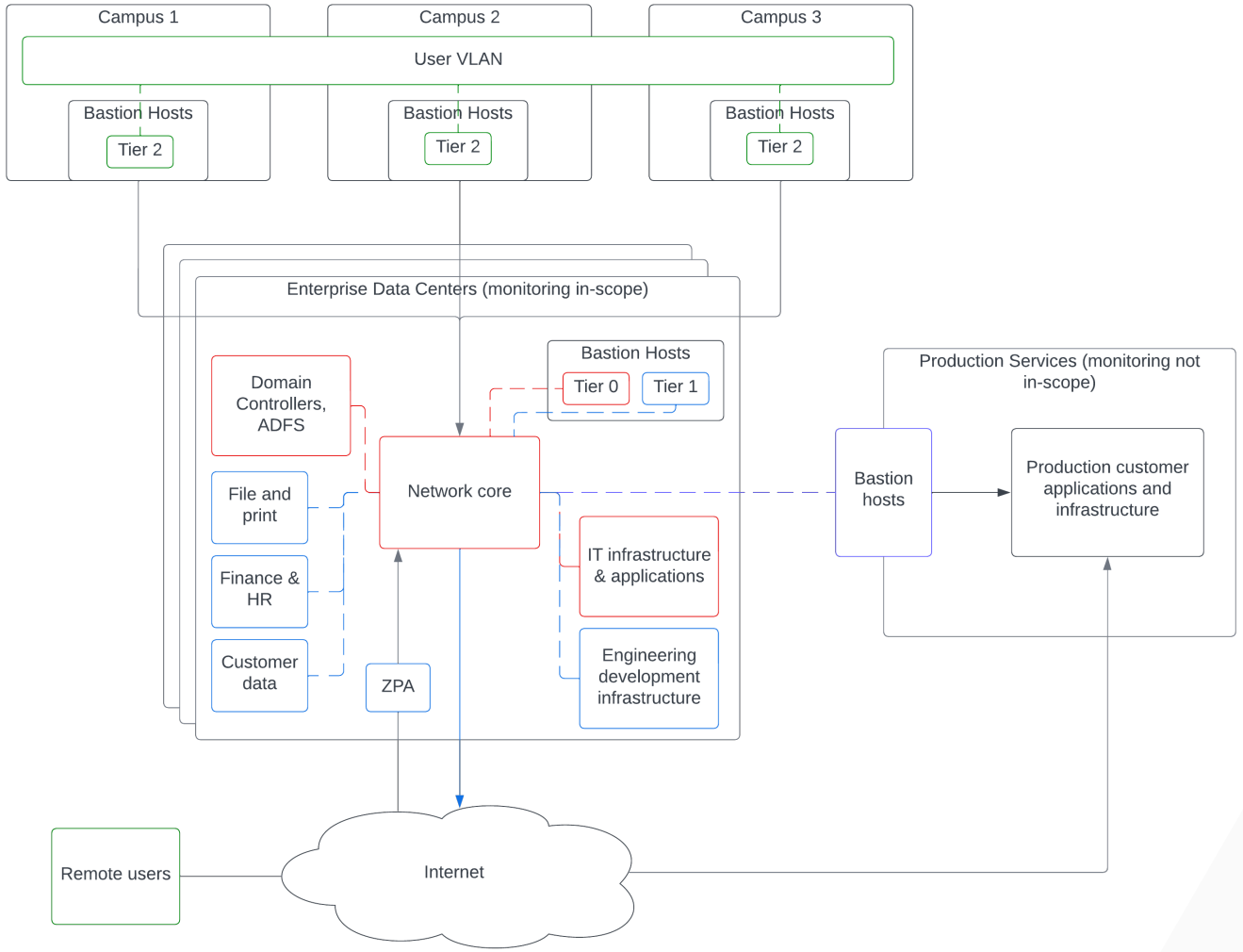
Example Environment Summary

Sources and Sinks

- Sources
  - Workstation VLAN (Tier 2)
  - Remote users / Zscaler ZPA
  - Trusted applications via supply chain risk
- Sinks
  - Enterprise IT Environment
    - File services, finance and HR applications
    - Customer resource management and customer data analytics
    - IT infrastructure and applications
    - Engineering development infrastructure
  - Production Services Environment
    - Engineering bastion hosts
    - Customer application data

Example Architectural Model

High-level overview of communication flows



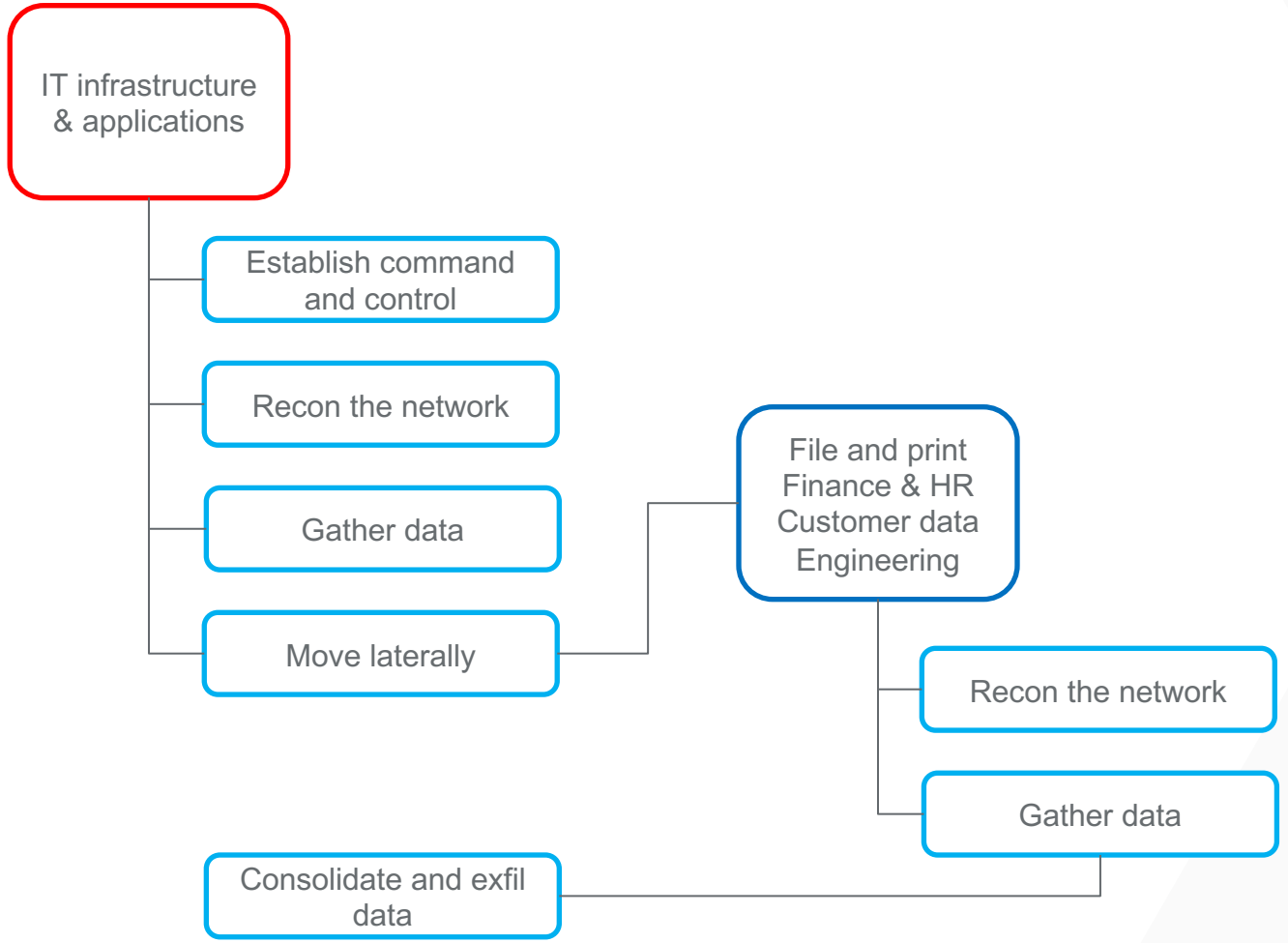
VECTRA
SECURITY THAT THINKS®

Rapid Threat Model Prototyping (RTMP) with MITRE ATT&CK

Analyze Threats

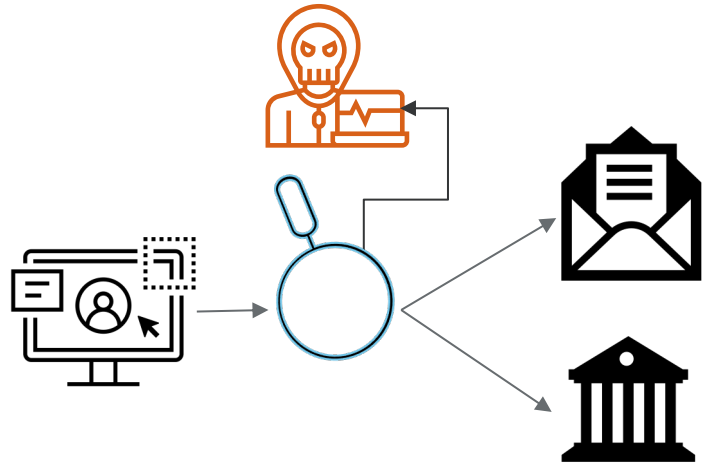
Attack Tree

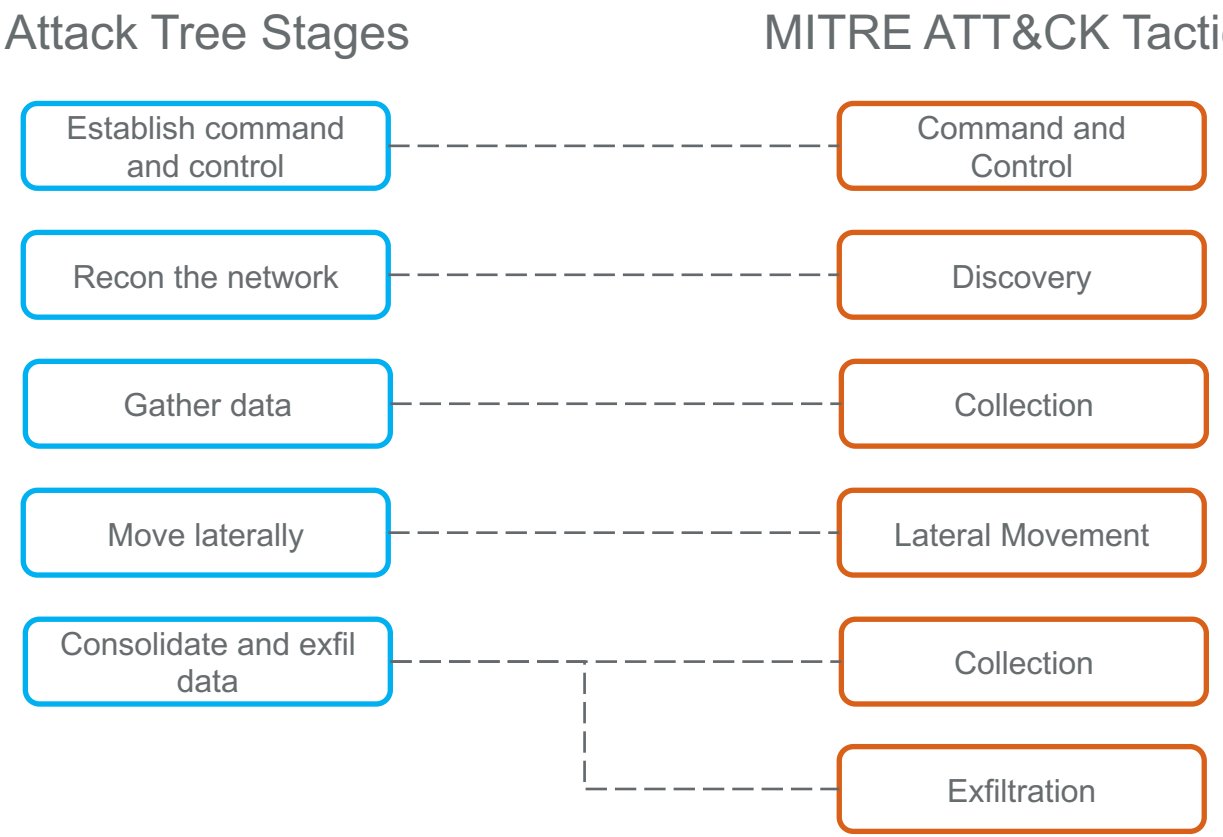
Supply chain attack originates from IT infrastructure



MITRE ATT&CK Tactics

- Attacker capabilities will be dependent on their reach and level of privilege in the environment





MITRE ATT&CK Techniques

Command and Control	Discovery	Collection	Lateral Movement	Exfiltration
Application Layer Protocol: • Web Protocols	**Account Discovery:** • Domain Account **Domain Trust Discovery** **Group Policy Discovery** **Network Service Discovery** **Network Share Discovery** **Remote System Discovery**	**Data from Information Repositories:** • Confluence • SharePoint • Code Repositories **Data from Network Shared Drive** **Data Staged:** • Local Data Staging	**Exploitation of Remote Services** **Remote Services:** • Remote Desktop Protocol • Windows Remote Management • Windows Management Instrumentation	**Exfiltration Over Alternative Protocol:** • Exfiltration Over Symmetric Encrypted Non-C2 Protocol • Exfiltration Over Asymmetric Encrypted Non-C2 Protocol • Exfiltration Over Unencrypted Non-C2 Protocol **Exfiltration Over C2 Channel** **Exfiltration Over Web Service:** • Exfiltration to Code Repository • Exfiltration to Cloud Storage • Exfiltration to Text Storage Sites

Rapid Threat Model Prototyping (RTMP) with MITRE ATT&CK

Analyze Mitigations

Mitigation Opportunities Summarized

Command and Control	Discovery	Collection	Lateral Movement	Exfiltration
Hidden Tunnel Detection	**Unusual LDAP queries**	**Large volumes of data being aggregated to a single internal host**	**Unusual WMI, RDP or WinRM activity between hosts**	**Large volumes of data leaving the environment after being staged internally**
Persistent connections to unusual domains	**Excessive RPC calls**	**Accessing fake shares/documents (traps triggered)**	**Attempted use of fake account credentials (traps triggered)**	
	RPC calls to key services			
	High volume of Kerberos ticket requests			
	SMB share enumeration			
	Access to fake ports / services (traps triggered)			
	Inquiry of fake accounts (traps triggered)			

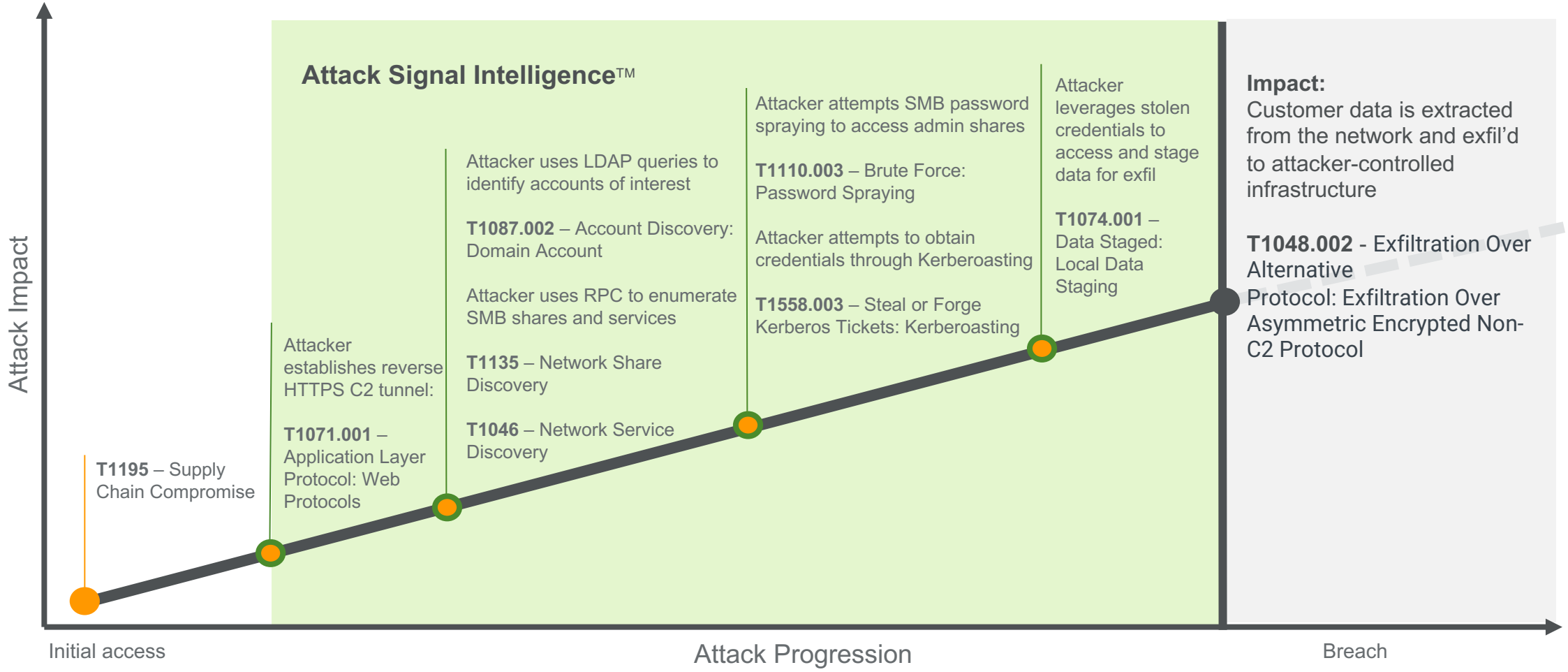
Rapid Threat Model Prototyping (RTMP) with MITRE ATT&CK

Validate

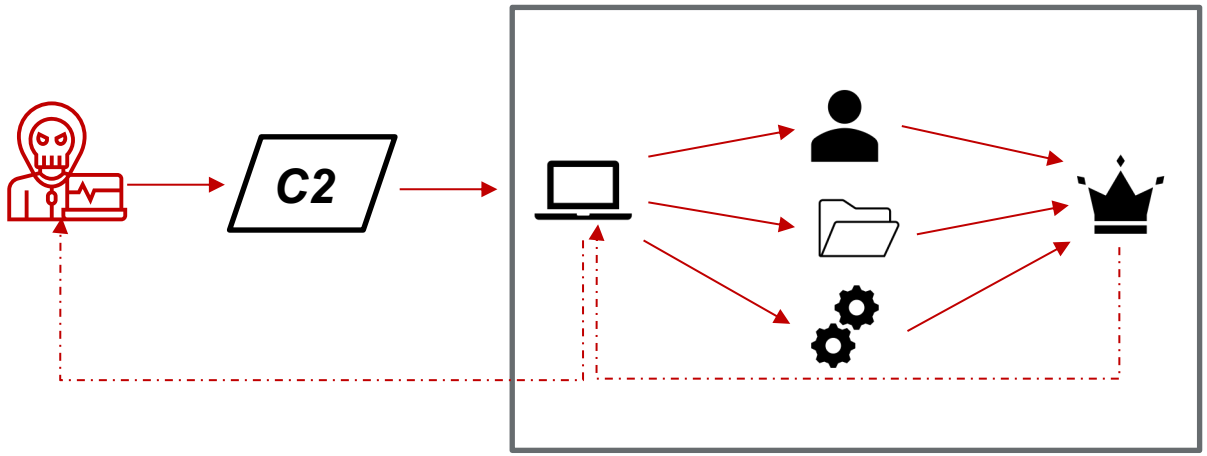
Attack Scenario

Initial access: APT instigated supply chain compromise

Objective: Acquire sensitive customer data



Attack Scenario Testing and Validation Timeline



Day 1: Initial Access

Launch **C2** on initial access host

Day 2: Discovery

Domain account, SMB share and service discovery

Day 3: Credential Access

Perform SMB **brute-force** and **Kerberoasting** to obtain privileged credentials

Day 4: Collection & Exfiltration

Collect, stage and exfil data to **attacker-controlled** infrastructure

Day 5+: Detection review

Confirm traffic flows, detections and notifications

Example Playbook Template

- This Post Compromise playbook is similar to the operations described in the attack scenario:
  - https://github.com/havocsh/havoc-labs/tree/main/custom_playbooks/post_compromise