

# Attack Flow Training: 4 – Visualization

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?

# What is Flow Visualization?

- Attack Flow is inherently visual – but a single mode of visualization.
- This might be limiting for certain audience or purposes.
- Flow Visualization* means to represent existing flows in new ways.

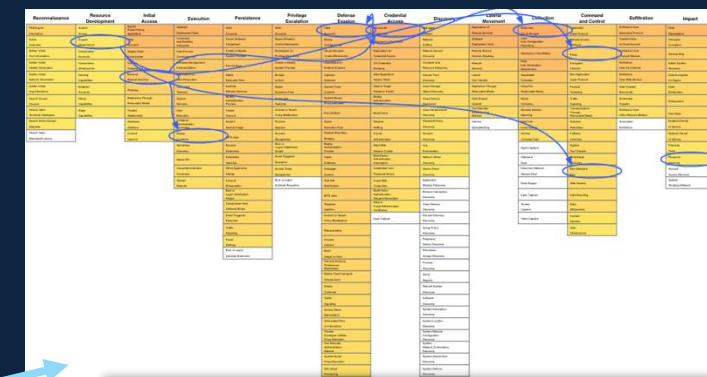
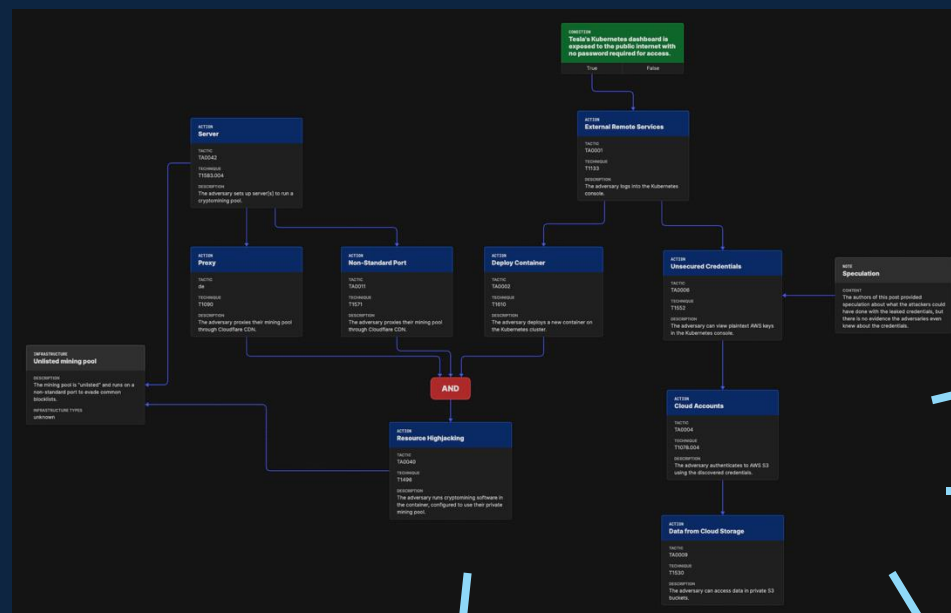


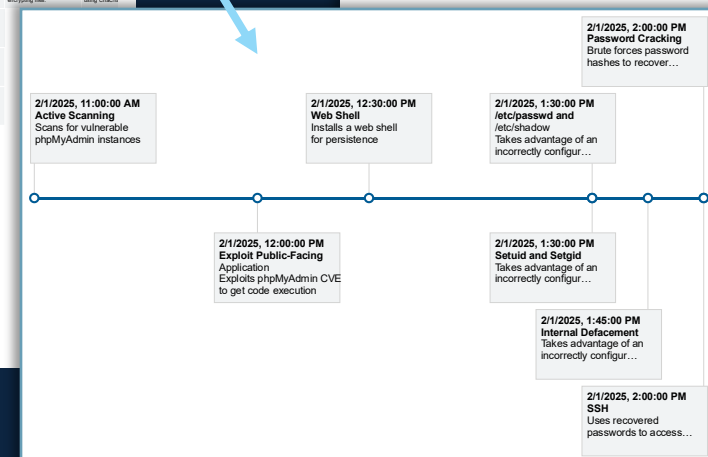
Table 1: TA0001 - Initial Access (Enterprise)

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.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Other
Phishing: Spearphishing Attachment - Victims receive spear phishing emails with malicious zip files attached.	User Execution: Malicious File - The zip files are extracted and usually contain a malicious document, such as a .doc, .pdf, or .xls.	Create Account: Accounts - Accounts are created with names such as temp, r, or admin.	System Services: Service Execution - Black Basta installs and uses PsExec to execute payloads on remote hosts.	Windows Management Instrumentation - Invoke-TotalExec is used to push out the ransomware binary.	Command and Scripting Interpreter: PowerShell - Within the malicious files, encoded PowerShell scripts are used to download additional malicious scripts.	System Information Discovery - The adversary runs system information software to discover system details.	Remote Services: Remote Desktop Protocol - RDP is used for lateral movement.	Analyze Collected Data - BlackBasta collects data from infected systems.	Remote Access: Software - Cobalt Strike is used for command and control communications.	Data Exfiltration: Data Exfiltration - The adversary exfiltrates data from the infected system.	



# Why Flow Visualization?

## Two Goals

### 1. Save time through automation

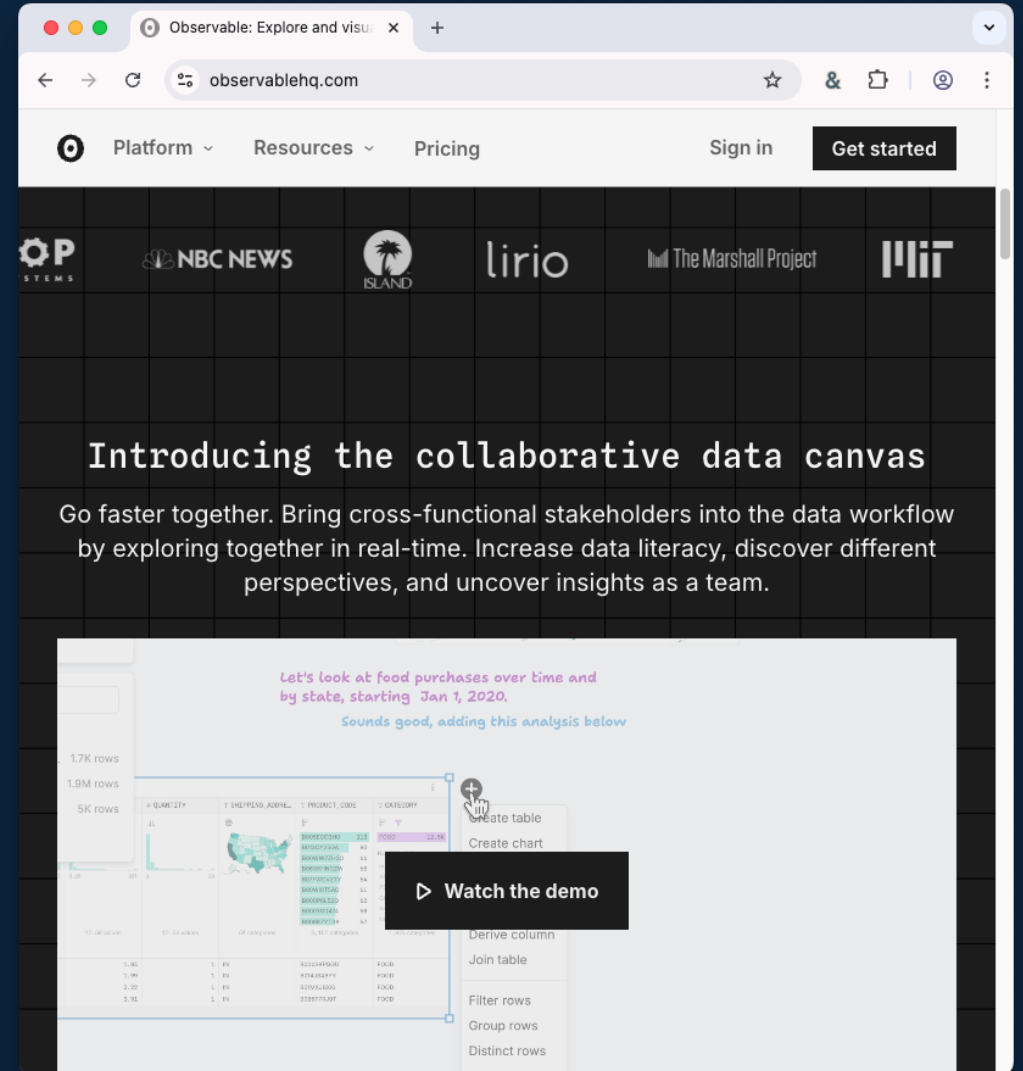
- Automate artifacts that are currently made by hand (or not at all)

### 2. Generate insights

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

# Using Visualization

- Visualizations are hosted on a platform called Observable that is separate from Attack Flow Builder.
- This allows us to try new things, take risks, and iterate quickly without diluting the quality of Attack Flow Builder.
- You can find a list of all the visualizations on the Attack Flow website.
- All the visualizations run in the browser and your data stays private.
- Go to <https://ctid.io/flow> and click “Visualization”



# Visualization: TTP Table

# TTP Table

October 16, 2024: Initial version.

## Appendix A: MITRE ATT&CK Tactics and Techniques

See **Tables 1–12** for all referenced actors' tactics and techniques in this advisory. For assistance with mapping malicious cyber activity to the MITRE ATT&CK framework, see CISA and MITRE ATT&CK's [Best Practices for MITRE ATT&CK Mapping](#) and CISA's [Decider Tool](#).

**Table 1: Reconnaissance**

Technique Title	ID	Use
Gather Victim Identity Information	<a href="#">T1589</a>	The actors likely gathered victim information.

**Table 2: Resource Development**

Technique Title	ID	Use
Obtain Capabilities: Tool	<a href="#">T1588.002</a>	The actors obtained a password spray tool through an open-source repository.

**Table 3: Initial Access**

Technique Title	ID	Use
Valid Accounts	<a href="#">T1078</a>	The actors used password spraying to obtain valid user and group email account credentials, allowing them access to the network.
Valid Accounts: Cloud Accounts	<a href="#">T1078.004</a>	The actors used accounts hosted on Microsoft 365, Azure, and Okta cloud environments as additional methods for initial access.
External Remote Services	<a href="#">T1133</a>	The actors exploited Citrix systems' external-facing remote services as another method for gaining initial access to the system.

**Table 4: Execution**

CISA often publishes a table of MITRE ATT&CK TTPs that summarizes an advisory.

# TTP Table

Flow Visualization  
generates a TTP table  
automatically from a flow.

Attack Flow: Tactic Table / MITRE

observablehq.com/d/010f86f3168a6b83

PlatformResourcesPricingSign inGet started

## How to Use It

First, open a flow in the Attack Flow Builder and choose "File → Publish Attack Flow" to save the flow in .json format. **Note that the flow must contain tactic and technique IDs.** Next, upload that .json file here to generate a tactic table.

Upload Attack Flow (.json)

Choose File

Black Bast...ware.json

Table header text#f1f3f4

Table header background#005b94

Copy table to clipboard

Copy Table

### 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.



**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.

**Table 3: TA0003 - Persistence (Enterprise)**

Technique Name	ATT&CK ID	Use
Create Account	T1136	Accounts are created with names such as temp, r, or admin.
Create or Modify System Process: Windows Service	T1543.003	Benign-looking services are created for the ransomware binary.

# TTP Table

**Table 1: TA0001 - Initial Access (Enterprise)**

Technique Name	ATT&CK ID	Use
Phishing: Spearphishing Attachment	<a href="#">T1566.001</a>	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	<a href="#">T1204.002</a>	The zip files are extracted and usually contain a malicious document, such as a .doc, .pdf, or .xls.
System Services: Service Execution	<a href="#">T1569.002</a>	Black Basta installs and uses PsExec to execute payloads on remote hosts.
Windows Management Instrumentation	<a href="#">T1047</a>	Invoke-TotalExec is used to push out the ransomware binary.
Command and Scripting Interpreter: PowerShell	<a href="#">T1059.001</a>	Within the malicious files, encoded PowerShell scripts are used to download additional malicious scripts.
Command and Scripting Interpreter: Visual Basic	<a href="#">T1059.005</a>	The extracted files contain malicious macros.

**Table 3: TA0003 - Persistence (Enterprise)**

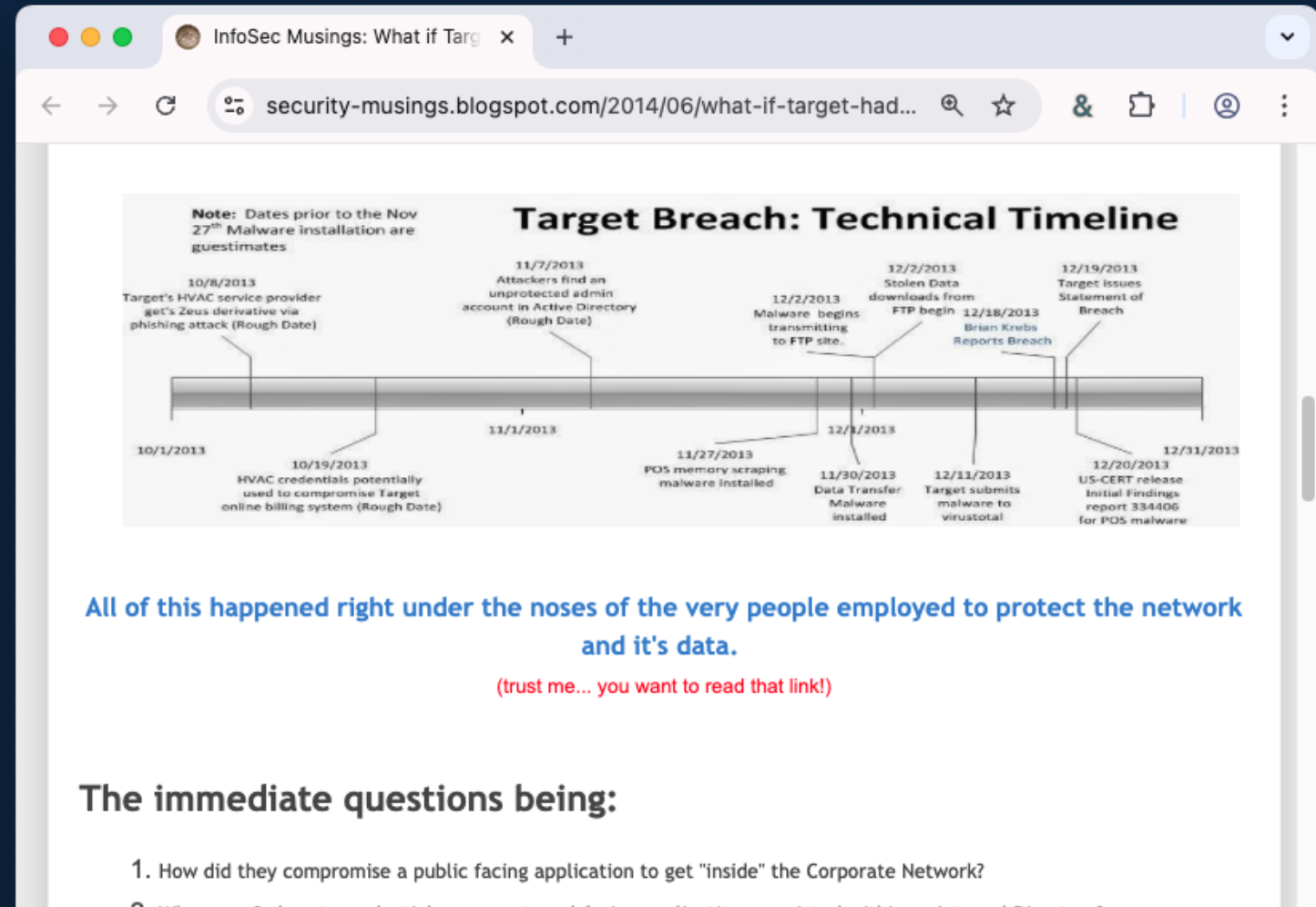
Technique Name	ATT&CK ID	Use
Create Account	<a href="#">T1136</a>	Accounts are created with names such as temp, r, or admin.
Create or Modify System Process: Windows Service	<a href="#">T1543.003</a>	Benign-looking services are created for the ransomware binary.

**Table 4: TA0004 - Privilege Escalation (Enterprise)**

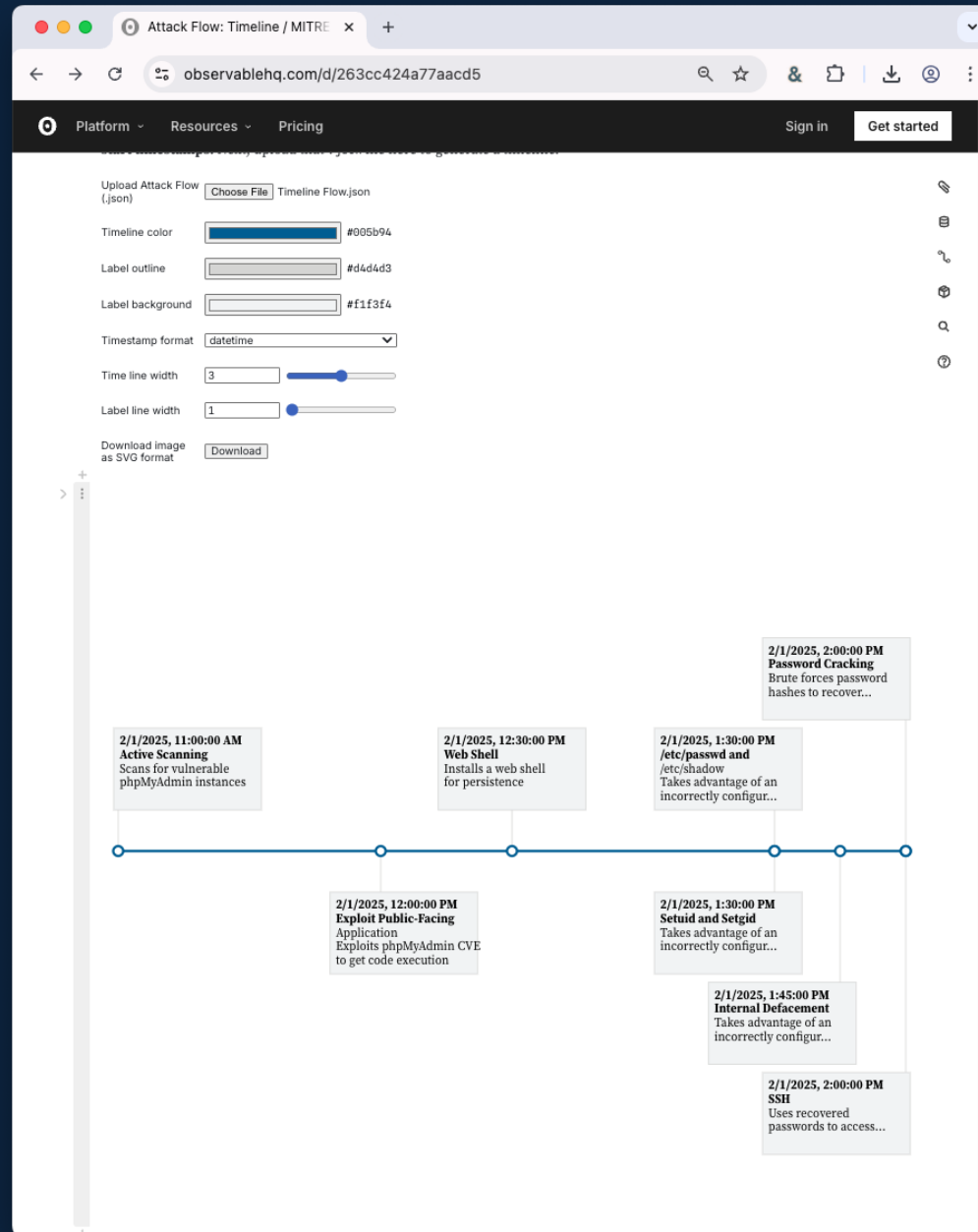
Copy and paste the table into a Word document or a web page.

# Timeline

Inspired by  
CTI reports  
that include a  
timeline of  
events.



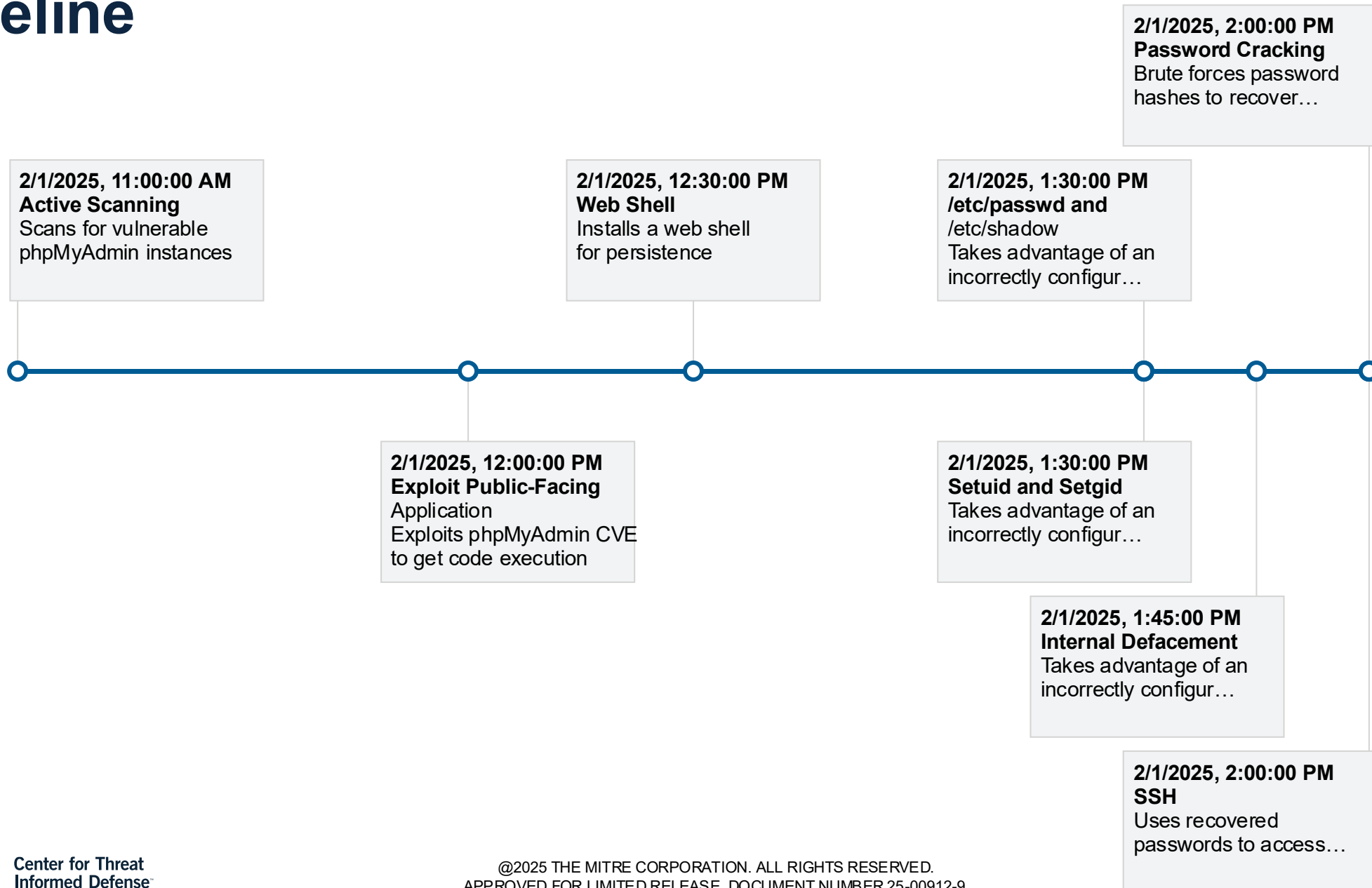
# Timeline



Turn a flow into a timeline. Download for use in presentations.

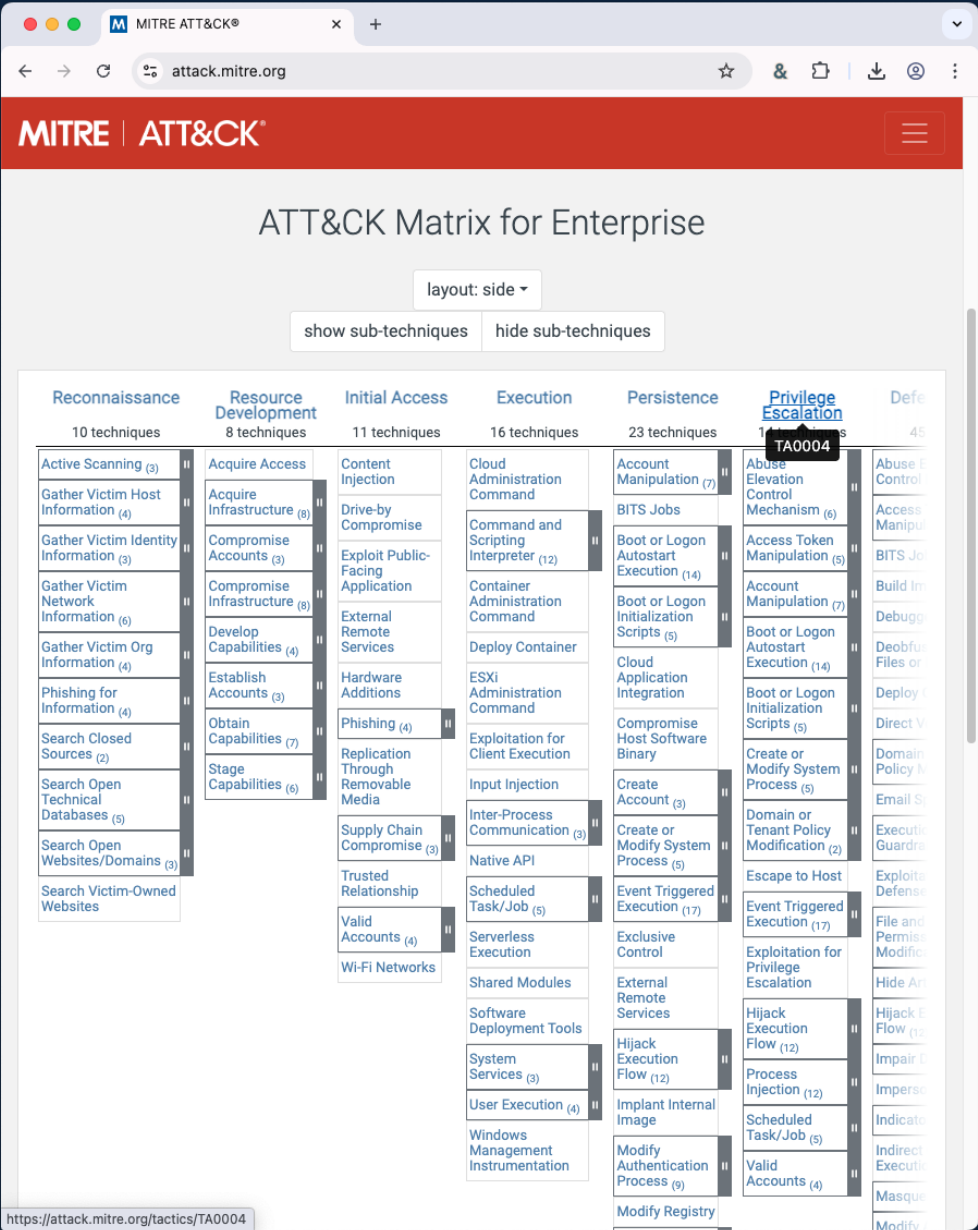
*The flow must contain execution timestamps.*

# Timeline



# Matrix

Inspired by the  
MITRE  
ATT&CK  
matrix.



# Matrix

PlatformResourcesPricingSign inGet started

MITRE Center for Threat-Informed Defense

UnlistedBy Mark E. HaaseEdited Apr 21

Attack Flow: Matrix View

TLP:AMBER:CTID-24-15

Distribution is limited to members in good standing of the Center for Threat-Informed Defense who are signatories to the Flow Visualization (24-15) project.

Introduction

On this page, you can generate an ATT&CK matrix automatically from an Attack Flow.

How to Use It

First, open a flow in the Attack Flow Builder and choose "File → Publish Attack Flow" to save the flow in .json format. **Note that the flow must contain tactic and technique IDs.** Next, upload that .json file here to generate a matrix view.

Upload Attack Flow (.json)

Choose File

Black Bast...ware.json

Download image as SVG format

Download Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	
Phishing: Spearphishing Attachment - Victims receive spear phishing emails with malicious zip files attached.	User Execution: Malicious File - The zip files are extracted and usually contain a malicious document, such as a d...	Create Account - Accounts are created with names such as temp, r, or admin.	Account Manipulation - The new accounts are added to the administrator's group to maintain elevated access.	System Binary Proxy Execution: Regsvr32 - regsvr32.exe is used to execute a malicious DLL	C S
	System Services: Service Execution - Black Basta installs and uses PsExec to execute payloads on remote hosts.	Create or Modify System Process: Windows Service - Benign-looking services are created for the ransomware binary.	Domain Policy Modification: Group Policy Modification - The Group Policy is modified for privilege escalati...	Indicator Removal on Host: File Deletion - BlackBasta attempts to delete malicious batch files.	
	Windows Management Instrumentation - Invoke-TotalExec is used to push out the ransomware binary.			Modify Registry - Modifications are made to the Registry.	
	Command and Scripting Interpreter: PowerShell - Within the malicious files, encoded PowerShell scripts are used to...			Deobfuscate/Decode Files or Information - Due to password protection, the zip files are able to bypass some AV detections.	
	Command and Scripting Interpreter: Visual Basic - The extracted files contain malicious macros.			Impair Defenses: Disable or Modify Tools - BlackBasta disables Windows Defender with batch scripts, such as...	
			Impair Defenses: Disable or Modify System Firewall - Batch scripts, such as rdp.bat or SERV1.bat, are used to modify the...		
			Impair Defenses: Safe Mode Boot - BlackBasta uses bcdedit to boot the device in safe mode.		

Group all the techniques in the flow into their corresponding tactics.

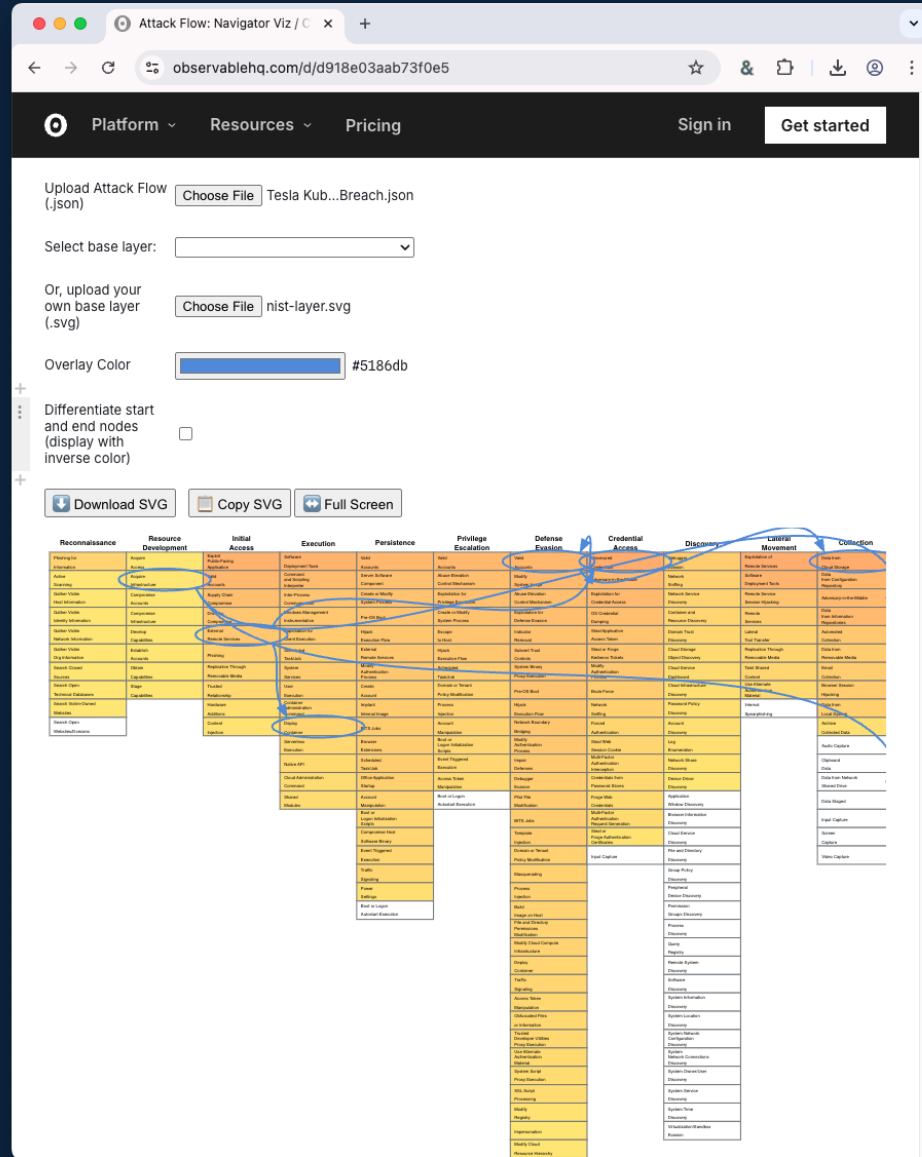
# Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Co
<b>Phishing: Spearphishing Attachment</b> – Victims receive spear phishing emails with malicious zip files attached.	<b>User Execution: Malicious File</b> – The zip files are extracted and usually contain a malicious document, such as a .d...	<b>Create Account – Accounts</b> are created with names such as temp, r, or admin.	<b>Account Manipulation</b> – The new accounts are added to the administrator's group to maintain elevated access.	<b>System Binary Proxy Execution: Regsvr32</b> – regsvr32.exe is used to execute a malicious DLL	<b>Credentials from Password Stores</b> – Mimikatz is used to dump passwords.	<b>Account Discovery: Domain Account</b> – Commands are used to discover domain account information.	<b>Remote Services: Remote Desktop Protocol</b> – RDP used for lateral movement.	<b>Archive Co</b> <b>Archive vi</b> – BlackBas data from i systems.
	<b>System Services: Service Execution – Black Basta</b> installs and uses PsExec to execute payloads on remote hosts.	<b>Create or Modify System Process: Windows Service</b> – Benign-looking services are created for the ransomware binary.	<b>Domain Policy Modification: Group Policy Modification</b> – The Group Policy is modified for privilege escalati...	<b>Indicator Removal on Host: File Deletion</b> – BlackBasta attempts to delete malicious batch files.		<b>System Network Configuration Discovery</b> – Attackers discovered internal IP addresses typically found on the...		
	<b>Windows Management Instrumentation</b> – Invoke-TotalExec is used to push out the ransomware binary.			<b>Modify Registry</b> – Modifications are made to the Registry.		<b>System Information Discovery</b> – GetComputerName is used to query to the computer name		
	<b>Command and Scripting Interpreter: PowerShell</b> – Within the malicious files, encoded PowerShell scripts are used to...			<b>Deobfuscate/Decode Files or Information</b> – Due to password protection, the zip files are able to bypass some AV detections.		<b>File and Directory Discovery</b> – Once booted in safe mode, BlackBasta will iterate through the entire file system		
	<b>Command and Scripting Interpreter: Visual Basic</b> – The extracted files contain malicious macros.			<b>Impair Defenses: Disable or Modify Tools</b> – BlackBasta disables Windows Defender with batch scripts, such as...				
				<b>Impair Defenses: Disable or Modify System Firewall</b> – Batch scripts, such as rdp.bat or SERVI.bat, are used to modify the...				
				<b>Impair Defenses: Safe Mode Boot</b> – BlackBasta uses bcdedit to boot the				



## Visualization: Navigator

# Mash up Attack Flow with an ATT&CK Navigator layer

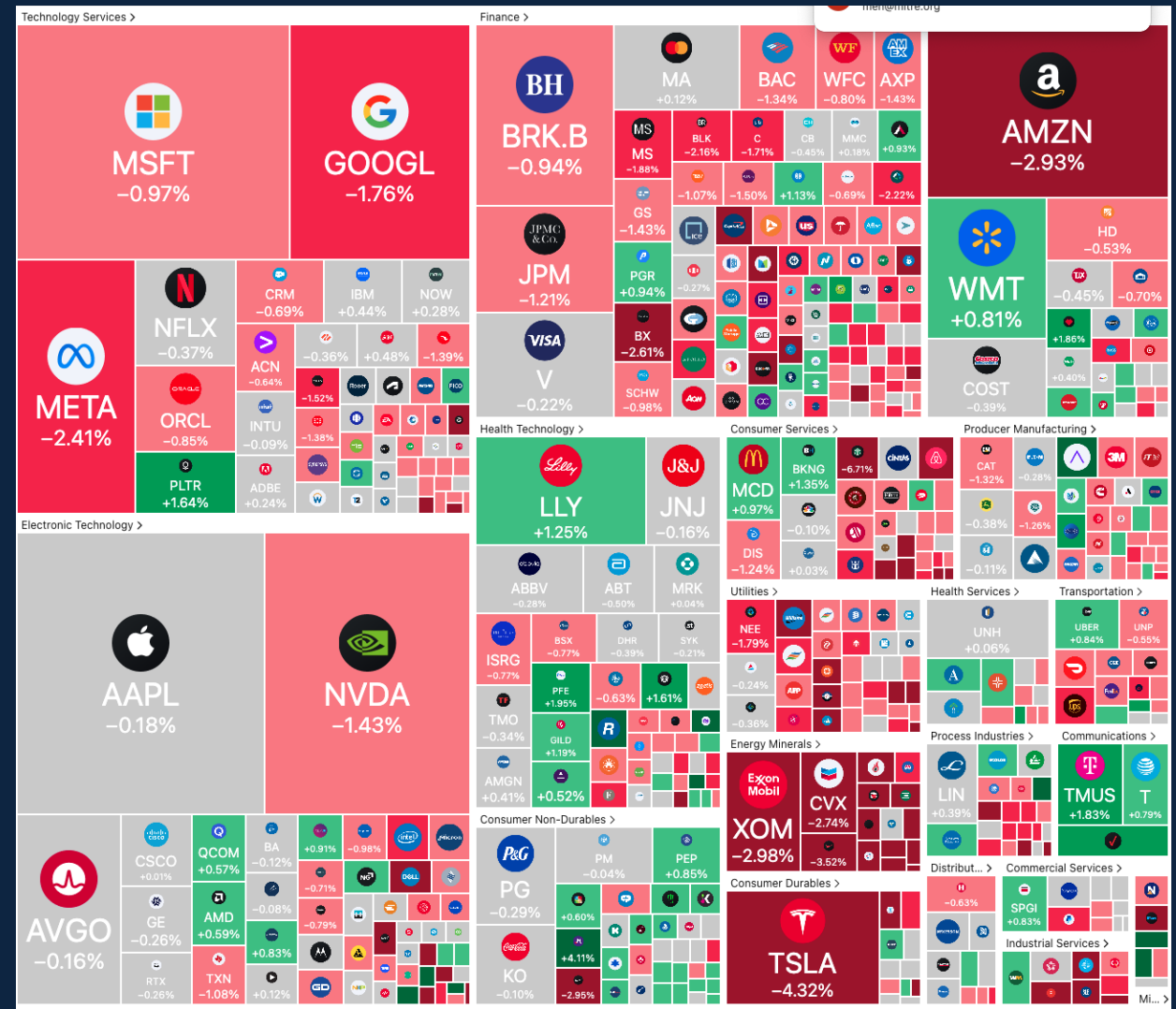


# Visualization: Navigator

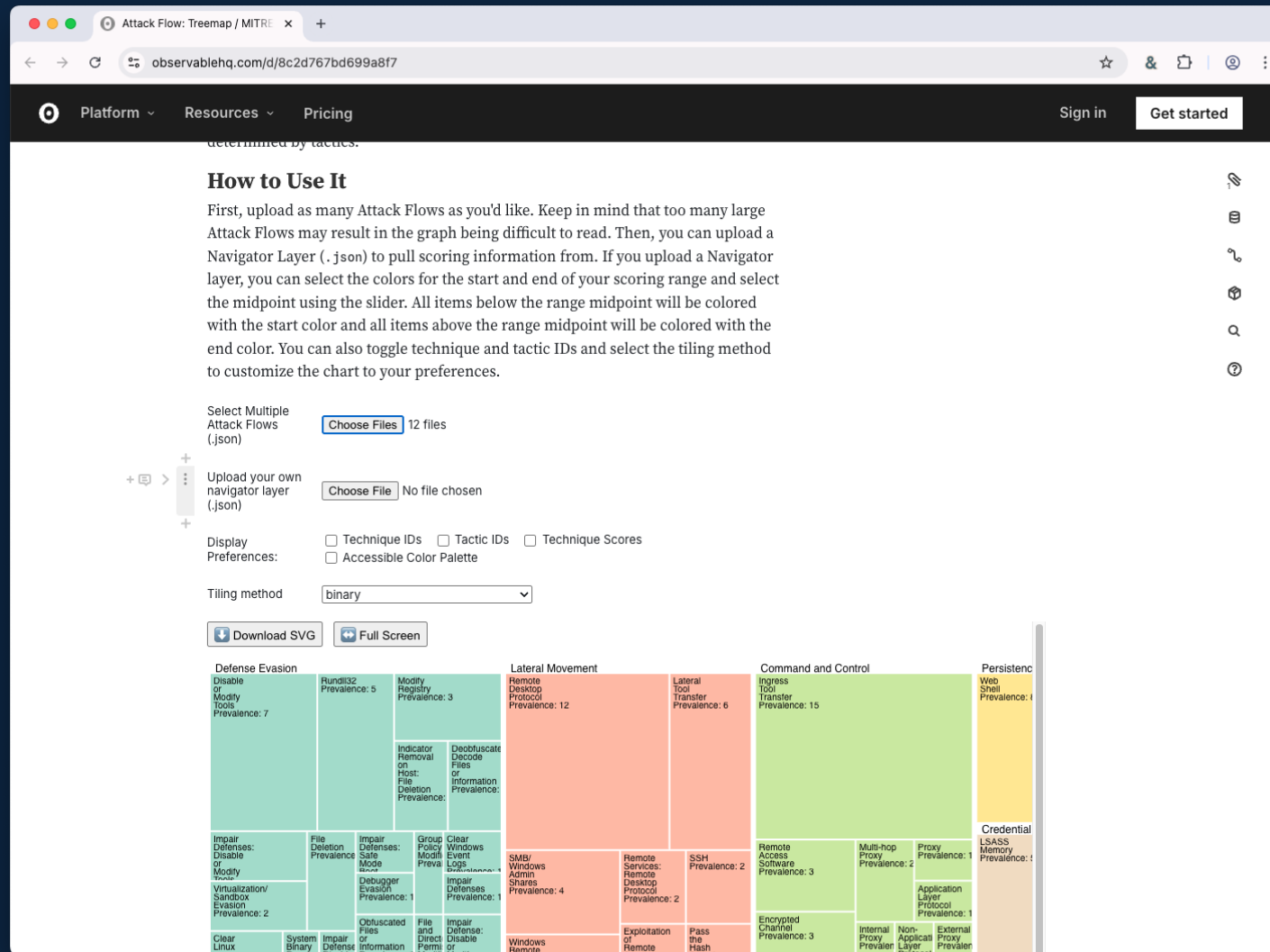
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
Phishing for Information	Acquire Access	Exploit Public-Facing Application	Software Deployment Tools	Valid Accounts	Valid Accounts	Valid Accounts	Insured Credentials
Active Scanning	Acquire Infrastructure	Valid Accounts	Command and Scripting Interpreter	Server Software Component	Abuse Elevation Control Mechanism	Modify System Image	Adversary-in-the-Middle
Gather Victim Host Information	Compromise Accounts	Supply Chain Compromise	Inter-Process Communication	Create or Modify System Process	Exploitation for Privilege Escalation	Abuse Elevation Control Mechanism	Exploitation for Credential Access
Gather Victim Identity Information	Compromise Infrastructure	Drive-by Compromise	Windows Management Instrumentation	Pre-OS Boot	Create or Modify System Process	Exploitation for Defense Evasion	OS Credential Dumping
Gather Victim Network Information	Develop Capabilities	External Remote Services	Exploitation for Client Execution	Hijack Execution Flow	Escape to Host	Indicator Removal	Steal Application Access Token
Gather Victim Organizational Information	Establish Accounts	Phishing	Scheduled Task/Job	External Remote Services	Hijack Execution Flow	Subvert Trust Controls	Steal or Forge Kerberos Tickets
Search Based Sources	Obtain Capabilities	Replication Through Removable Media	System Services	Modify Authentication Process	Scheduled Task/Job	System Binary Proxy Execution	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 Web sites		Hardware Additions	Container Administration Command	Implement Internal Image	Process Injection	Hijack Execution Flow	Network Sniffing
Search Open Web sites/Domains		Content Injection	Deploy Container	PTS Jobs	Account Manipulation	Network Boundary Bridging	Forced Authentication
			Serverless Execution	Browser Extensions	Boot or Logon Initialization Scripts	Modify Authentication Process	Steal Web Session Cookie
			Native API	Scheduled Task/Job	Event Triggered Execution	Impair Defenses	Multi-Factor Authentication Interception
			Cloud Administration Command	Office Application Startup	Access Token Manipulation	Debugger Evasion	Credentials from Password Stores

# Visualization: Tree Map

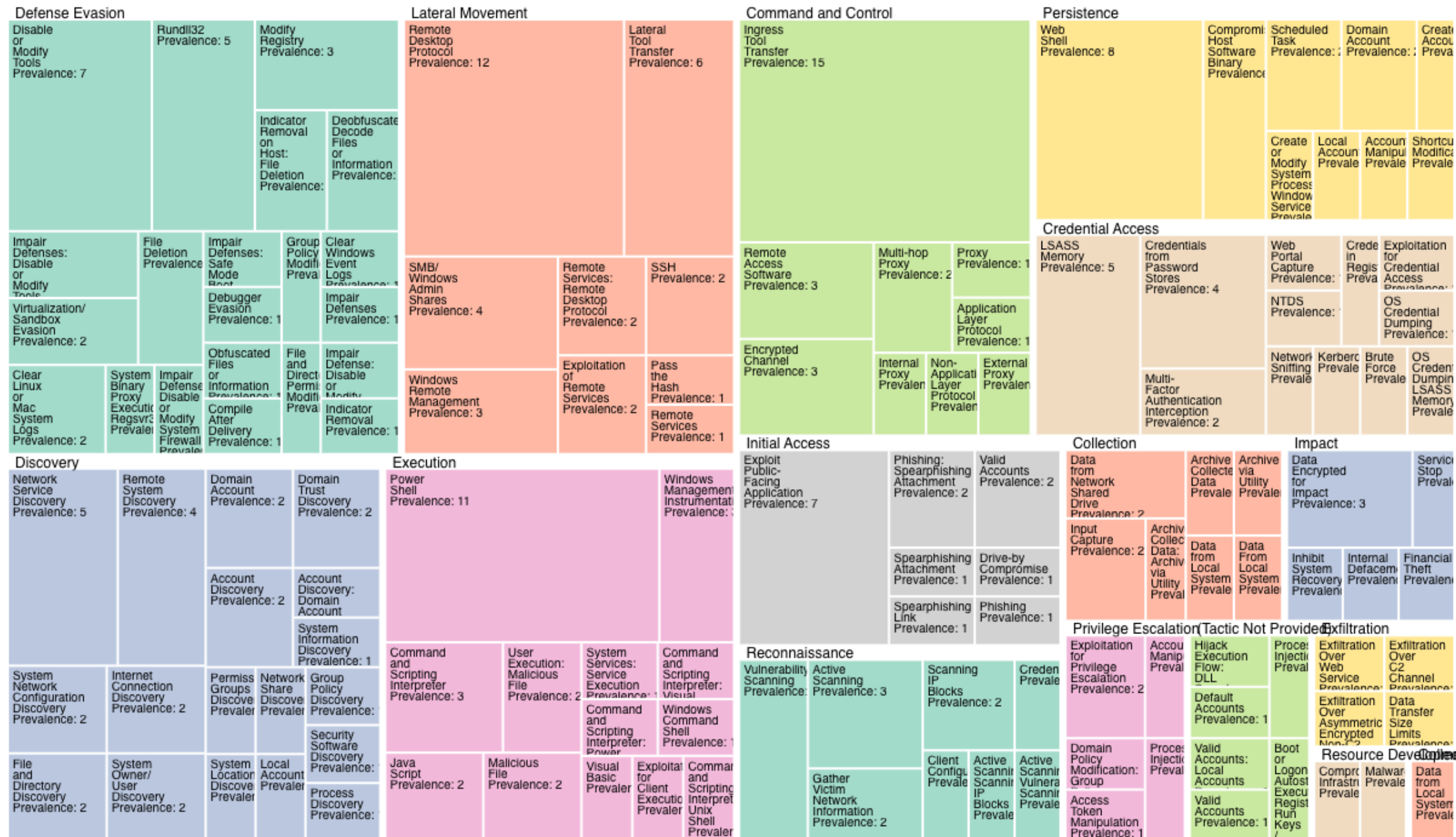
Inspired by this stock market visualization that shows market activity by sector.



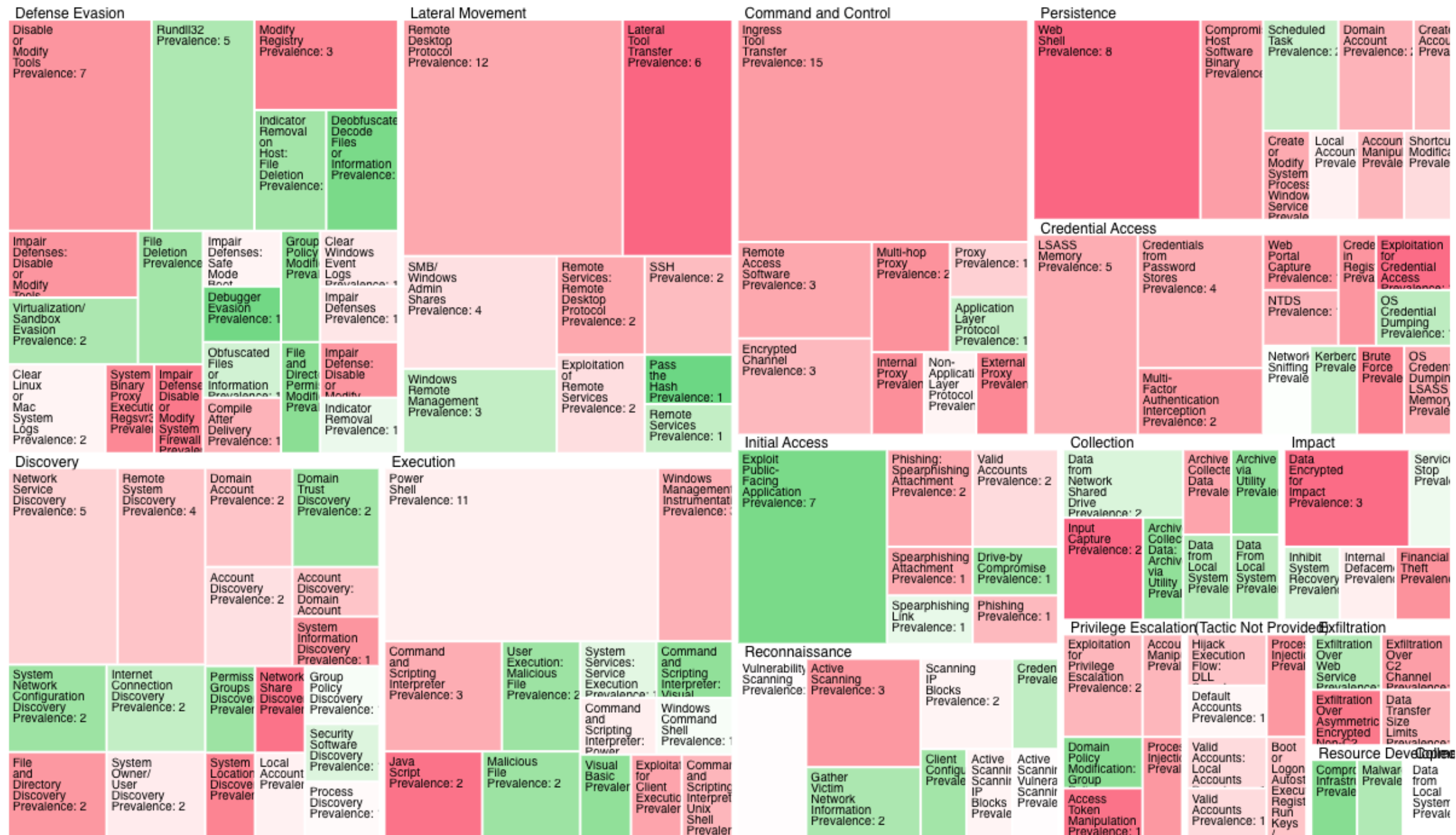
# Visualization: Tree Map



The treemap view aggregates data across multiple flows.







# Demo

# End of Section 4