



TIE IN THREATS TOGETHE

BY APPLYING THE TECHNIQUE INFERENCE
R... LINE TO ENHANCE DETECTIONS





RAYMOND
SCHIPPERS

INTRO RAYMOND

- CTO/CISO @ Huntabil.IT
- Previously Engineering Director - Cyber Defence @ Canva
- 15+ years in cyber defence and CTI roles

Graphics where generated by Leonardo.AI

INTRODUCTI SECURIT

Y

In a galaxy close to all of us...

in a time no so distant...

We are here to understand our adversaries
and use our Jedi powers to predict their next moves



CYBE GALAXY

R



ADVERSARIES

The threats we look to do battle with on a daily basis



TECHNIQUES

How our adversaries go about their deeds, the methods they use to attack us



JEDIS

We the defenders, fightings against evil naydoers



TECHNIQUE INFERENCE ENGINE OUR JEDI POWER

Graph-based system taught to
understand connections between
TTPs

WHY USE TIE



CHALLENGE

Incomplete adversary reporting,

SOLUTION

Make predictions on likely TTPs to fill in the gaps.



EXAMPLE SCENARIO 1

Reports on the compromise of a peer in our industry.

We know actions on objective and some other details but we don't know:

- How did they get in
- what are their possible lateral movement steps?
- What detections should we have?

OBSERVED TECHNIQUES

ADD TECHNIQUE



↑ .CSV

> T1486:
DATA ENCRYPTED FOR IMPACT



> T1566:
PHISHING



DEMO SCENARIO 1

Add observed techniques

Then add techniques it returns to refine the model

When it makes sense, export the layer

↕ ORGANIZE

≡ FILTER

↓ NAVIGATOR LAYER

↓ .CSV

Execution

> T1059:
COMMAND AND SCRIPTING INTERPRETER

#1



> T1059.001:
POWERSHELL

#5



> T1053:
SCHEDULED TASK/JOB

#8



> T1204:
USER EXECUTION

#10



> T1047:
WINDOWS MANAGEMENT INSTRUMENTATION

#13



DEMO

SCENARIO 1

The heatmap shows you confidence of the techniques used

Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 17 techniques	Exfiltration 9 techniques
Exploit Public-Facing Application	Command and Scripting Interpreter (1/9)	Boot or Logon Autostart Execution (0/14)	Boot or Logon Autostart Execution (0/14)	Masquerading (0/9)	OS Credential Dumping (0/8)	Account Discovery (0/4)	Remote Services (0/8)	Input Capture (0/4)	Web Service (0/3)	Automated Exfiltration (0/1)
Valid Accounts (0/4)	User Execution (1/3)	Scheduled Task/Job (0/5)	Process Injection (0/12)	Process Injection (0/12)	Input Capture (0/4)	Application Window Discovery	Exploitation of Remote Services	Adversary-in-the-Middle (0/3)	Proxy (0/4)	Data Transfer (0/1)
Content Injection	Scheduled Task/Job (0/5)	Valid Accounts (0/4)	Scheduled Task/Job (0/5)	Valid Accounts (0/4)	Adversary-in-the-Middle (0/3)	Browser Information Discovery	Internal Spearphishing	Archive Collected Data (0/3)	Application Layer Protocol (0/4)	Exfiltration (0/2)
Drive-by Compromise	Cloud Administration Command	Account Manipulation (0/6)	Valid Accounts (0/4)	System Binary Proxy Execution (0/13)	Brute Force (0/4)	Cloud Infrastructure Discovery	Lateral Tool Transfer	Audio Capture	Communication Through Removable Media	Exfiltration (0/2)
External Remote Services	Container Administration Command	BITS Jobs	Abuse Elevation Control Mechanism (0/5)	Indicator Removal (0/9)	Credentials from Password Stores (0/6)	Cloud Service Dashboard	Remote Service Session Hijacking (0/2)	Automated Collection	Content Injection	Exfiltration (0/2)
Hardware Additions	Deploy Container	Boot or Logon Initialization Scripts (0/5)	Access Token Manipulation (0/5)	Abuse Elevation Control Mechanism (0/5)	Exploitation for Credential Access	Cloud Service Discovery	Replication Through Removable Media	Browser Session Hijacking	Data Encoding (0/2)	Exfiltration (0/1)
Phishing (2/4)	Exploitation for Client Execution	Browser Extensions	Account Manipulation (0/6)	Access Token Manipulation (0/5)	Forced Authentication	Cloud Storage Object Discovery	Software Deployment Tools	Clipboard Data	Data Obfuscation (0/3)	Exfiltration (0/1)
Replication Through Removable Media	Inter-Process Communication (0/3)	Compromise Client Software Binary	Boot or Logon Initialization Scripts (0/5)	BITS Jobs	Forge Web Credentials (0/2)	Container and Resource Discovery	Taint Shared Content	Data from Cloud Storage	Dynamic Resolution (0/3)	Exfiltration (0/4)
Supply Chain Compromise	Native API	Create Account		Debugger Evasion	Modify Authentication Process	Debugger Evasion	Use Alternate Authentication Material	Data from Configuration Repository (0/2)	Encrypted Channel (0/2)	Scheduled Exfiltration (0/1)
						Device Driver Discovery		Data from Information	Fallback Channels	

CHALLENGE

The need to create realistic possible adversary profiles based on a set of TTPs

SOLUTION

TIE lets you create highly probable adversaries based on known real world attacks

WHY USE TIE



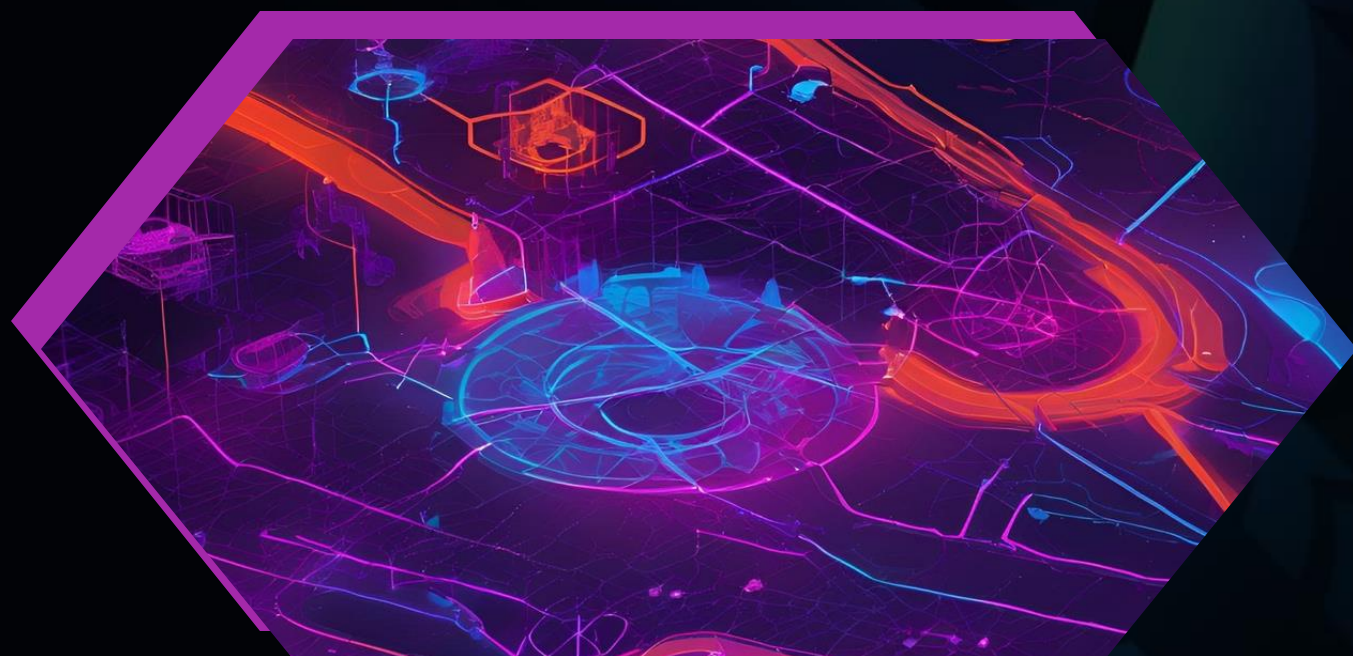


EXAMPLE SCENARIO 2

We need to simulate & creates detections for an adversary likely to steal data from a S3 bucket through stolen credentials.

TIE can help us create a likely adversary profile with TTPs

USING FORCE



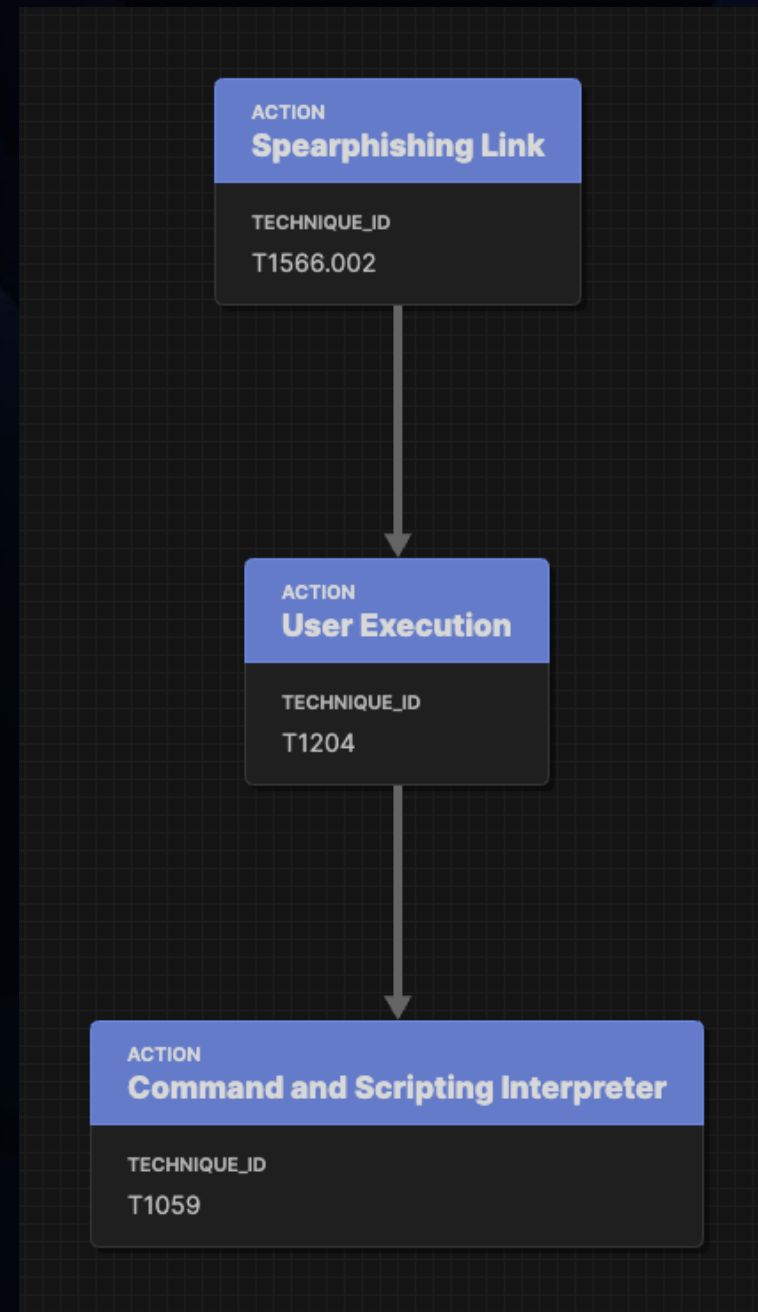


BUILDING KNOWLEDG

- E** Feed into TTPs into the rest of the Threat informed defence cycle
- Help build adversary profiles
 - Improve your adversary simulations and develop likely adversaries to simulate

BUILDING KNOWLEDG

- E** What are our courses of action for these techniques
- Help build better ATT&CK Flows
 - See common choke points





DETECTI REQUIREME NTS

- Build a comprehensive list of likely TTP
- Build attack flows
- Look for top-N detections
- Prioritise based on the clusters
- Use Summing the Pyramid to factor in resilience



Unique Inference Engine (TIE) Prediction Heatmap X Technique Inference Engine (TIE) Prediction Heatmap X layer by operation X +						
Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques
Content Injection	Cloud Administration Command	Account Manipulation (0/5)	Abuse Elevation Control Mechanism (0/5)	Abuse Elevation Control Mechanism (0/5)	Adversary-in-the-Middle (0/3)	Account Discovery (0/4)
Drive-by Compromise	Command and Scripting Interpreter (1/9)	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery
Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (0/4)	Account Manipulation (0/5)	BITS Jobs	Credentials from Password Stores (0/5)	Browser Information Discovery
External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Autostart Execution (0/4)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery
Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (0/5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard
Phishing (2/4)	Inter-Process Communication (0/3)	Compromise Client Software Binary	Create or Modify System Process (0/4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (0/2)	Cloud Service Discovery
Replication Through Removable Media	Native API	Create Account (0/3)	Domain Policy Modification (0/2)	Deploy Container	Input Capture (0/4)	Cloud Storage Object Discovery
Supply Chain Compromise (0/3)	Scheduled Task/Job (0/5)	Create or Modify System Process (0/4)	Event Triggered Execution (0/18)	Direct Volume Access	Modify Authentication Process (0/8)	Container and Resource Discovery
Trusted Relationship	Serverless Execution	Event Triggered Execution (0/18)	Escape to Host	Domain Policy Modification (0/2)	Multi-Factor Authentication Interception	Debugger Evasion
Valid Accounts (0/4)	Shared Modules	External Remote Services	Event Triggered Execution (0/18)	Execution Guardrails (0/1)	Multi-Factor Authentication Request Generation	Device Driver Discovery
	Software Deployment Tools	Hijack Execution Flow (0/12)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Network Sniffing	Domain Trust Discovery
	System Services (0/2)	Implant Internal Image	Hijack Execution Flow (0/12)	File and Directory Permissions Modification (0/2)	OS Credential Dumping (0/8)	File and Directory Discovery
	User Execution (1/3)	Modify Authentication Process (0/5)	Process Injection (0/12)	Hide Artifacts (0/11)	Steal Application Access Token	Group Policy Discovery
	Windows Management Instrumentation	Office Application Startup (0/5)	Scheduled Task/Job (0/5)	Hijack Execution Flow (0/12)	Steal or Forge Authentication Certificates	Log Enumeration
		Power Settings	Valid Accounts (0/4)	Impair Defenses (0/11)	Steal or Forge Kerberos Tickets (0/4)	Network Service Discovery
		Pre-OS Boot (0/5)		Impersonation	Steal Web Session Cookie	Network Share Discovery
		Scheduled Task/Job (0/5)		Indicator Removal (0/9)	Unsecured Credentials (0/8)	Network Sniffing
		Server Software Component (0/5)		Indirect Command Execution		Password Policy Discovery
		Traffic Signaling (0/2)		Masquerading (0/6)		Peripheral Device Discovery
		Valid Accounts (0/4)		Modify Authentication Process (0/8)		Permission Groups Discovery (0/3)
				Modify Cloud Compute Infrastructure (0/5)		Process Discovery
				Modify Registry		Query Registry
				Modify System Image (0/2)		Remote System Discovery
				Network Boundary Bridging (0/1)		Software Discovery (0/1)
				Obfuscated Files or Information (0/12)		System Information Discovery
				Plist File Modification		System Location Discovery (0/1)
				Pre-OS Boot (0/5)		System Network Configuration Discovery (0/2)
				Process Injection (0/12)		System Network Connections Discovery
				Reflective Code Loading		System Owner/User Discovery
				Rogue Domain Controller		System Service Discovery
				Rootkit		System Time Discovery
				Subvert Trust Controls (0/8)		Virtualization/Sandbox Evasion (0/3)
				System Binary Proxy Execution (0/13)		
				System Service Binary Execution		

DETECT REQUIREMENTS

- Build your ATT&CK Layers
- Import them into navigator
 - Add A+B+C etc
 - Use the heatmap generated



DETECTI IDEAS

- Understand what is likely left of boom
- Build comprehensive understanding of post-compromise pre-impact TTPs
- Increase confidence of CTI based prioritisations



ADVERSAR SIMULATION

- Build more completed profiles
- Build potential profiles to simulate
- Help create attack flows
- Import into tools like OpenBAS



THE STRATEGY

- Leverage TIE to enhance CTI reporting
- Build profiles to simulate likely new adversaries
- Enhance your resilience and feed into the other great projects from MITRE



CHALLENGE WITH TIE

- Uses ATT&CK V14
- Common techniques have been renumbered so dataset is..challenging
- You can't select appropriate platforms
- Can't export from TIE>ATT&CK Flow



TIEING IT TOGETHER

As community let's contribute

adversary knowledge

- Let's use our Jedi powers for good
- Join the defence alliance
- MITRE, how can we continue to improve the model as a community?
- MITRE: Let me select appropriate platforms

QUESTION

S?



THANK YOU



My LinkedIn



MITRE ATT&CK
Slack

**LET'S
NONE OF US
ARE AS
KNOWLEDGEAB
LE AS ALL OF
US**