

# Decoding Cyber Threats

A Practical Guide to Using Attack Trees

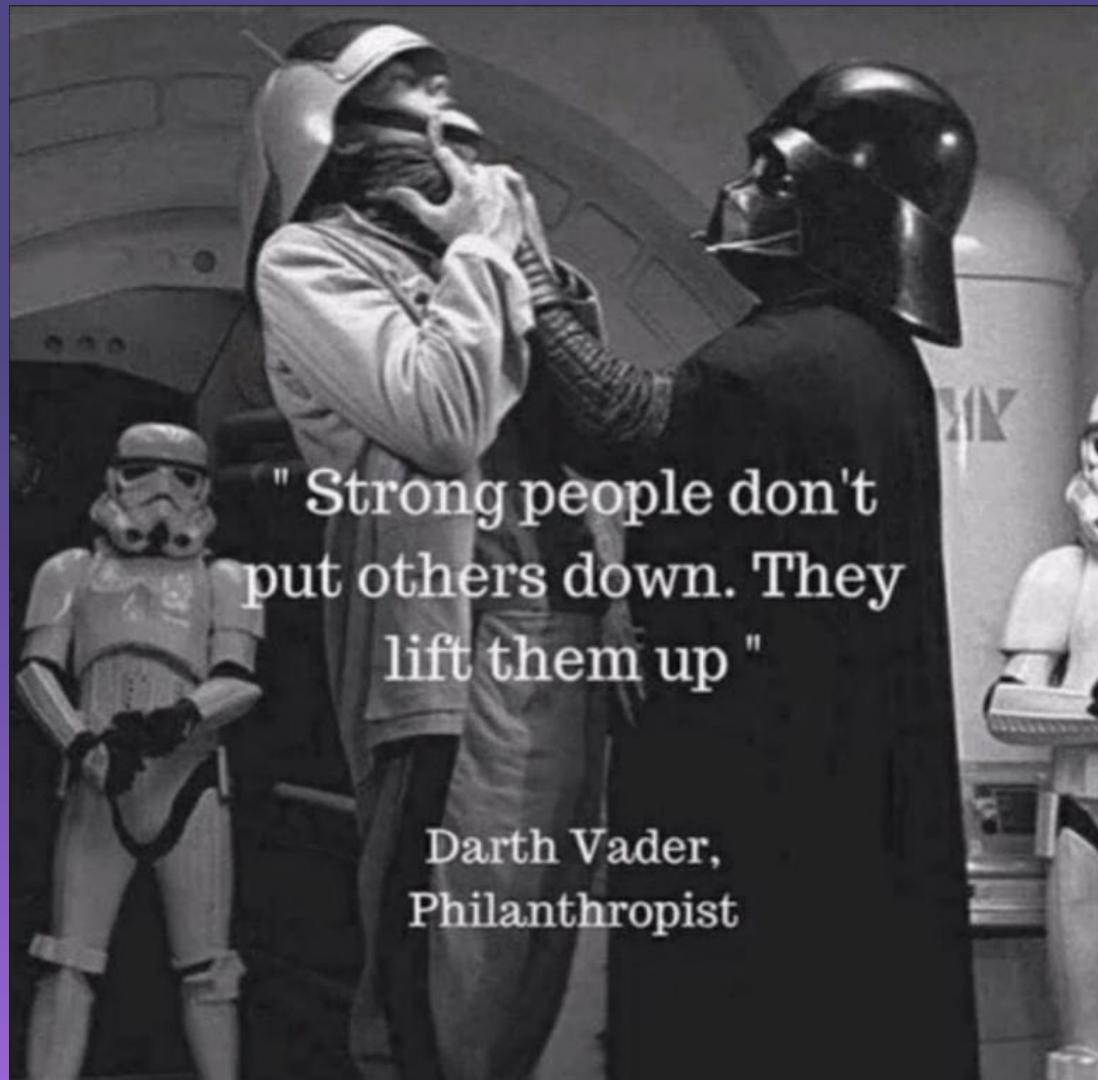
Gert-Jan Bruggink & Sherman Chu

28 January 2025



...

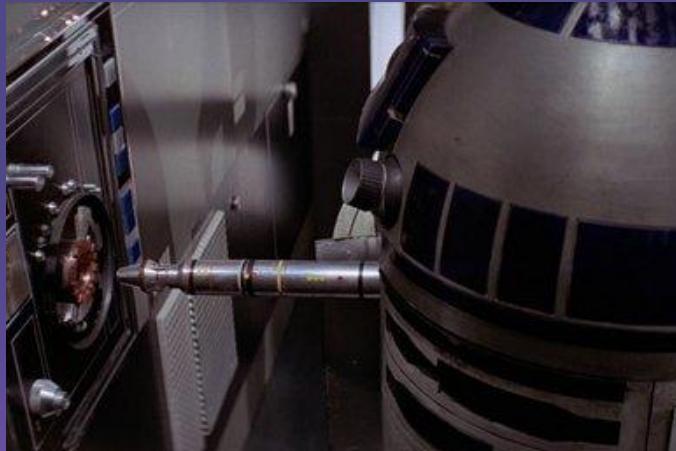
# CTI & Decision-Making





...

# Ever been in this situation?



Identifying  
Systemic  
Vulnerabilities

Responding  
to an Incident

Prioritizing  
Security  
Investment



# ... Sometimes while protecting your business, you need to make rapid decisions

Would be real bad  
if something  
happened to it.

Yeah boss,  
totally.

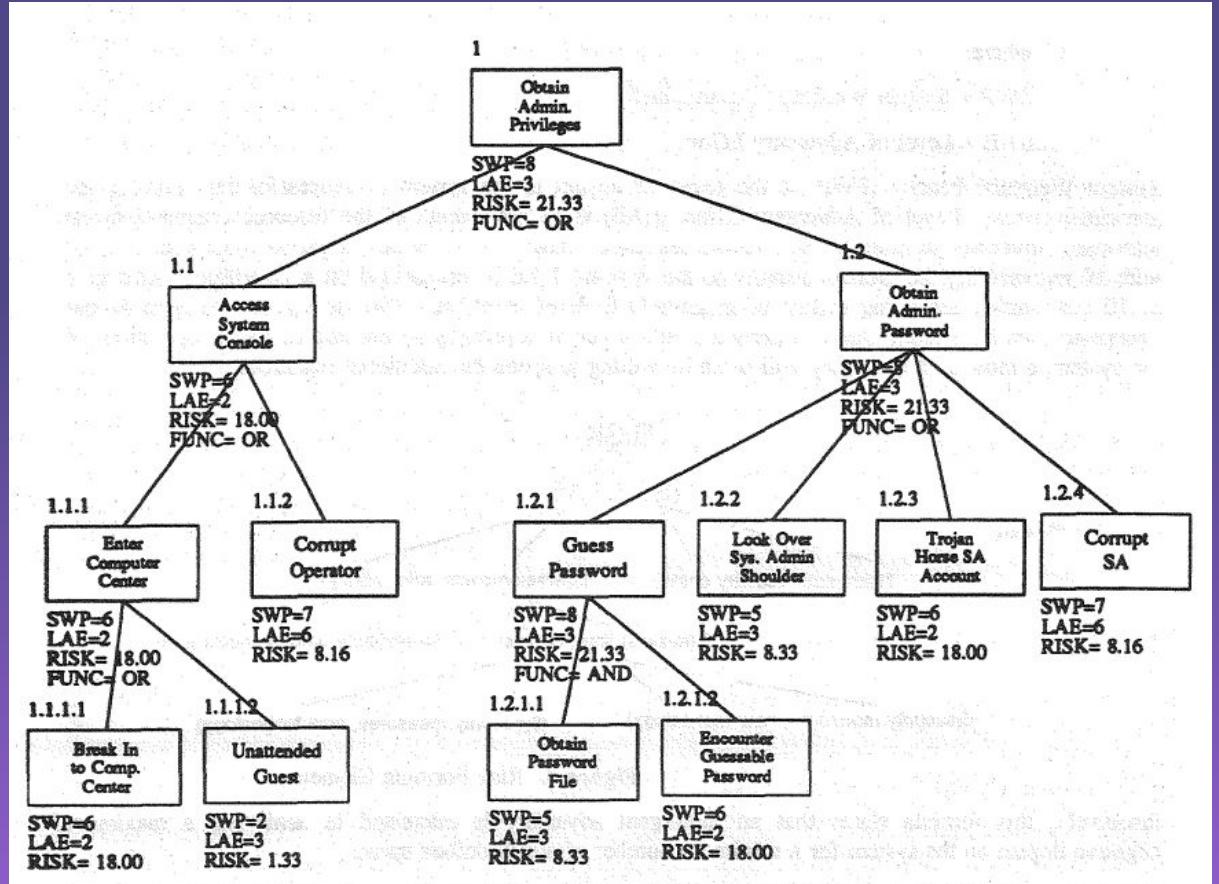


# Why Attack Trees



# Why were Attack Trees created in the first place?

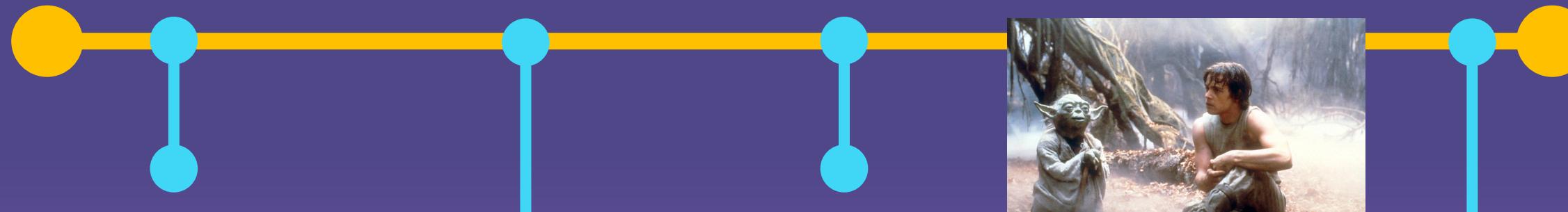
- Visualize Attack Scenarios
- Threat Modeling
- Decision-Making



*Jonathan Weiss, 1982*



# We love history



**1982**  
Conceptualized  
as threat trees  
by Jonathan  
Weiss, Bell  
laboratories

**1999**  
Bruce Schneier  
publishes attack  
tree concepts

**2013**  
Diamond Model  
of Intrusion  
incorporates  
attack tree  
attributes

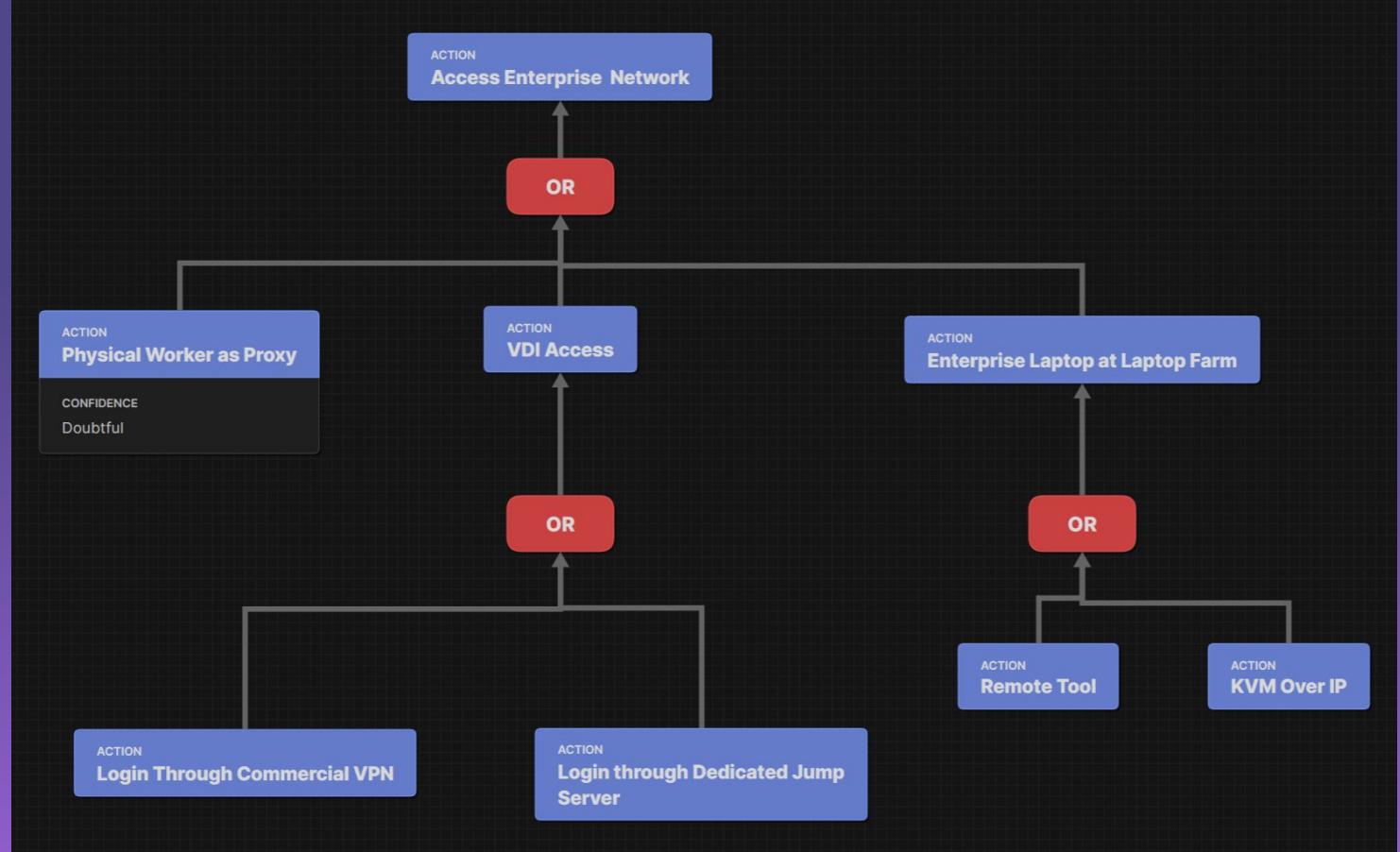


**2025**  
Two nerds at CTI  
conference



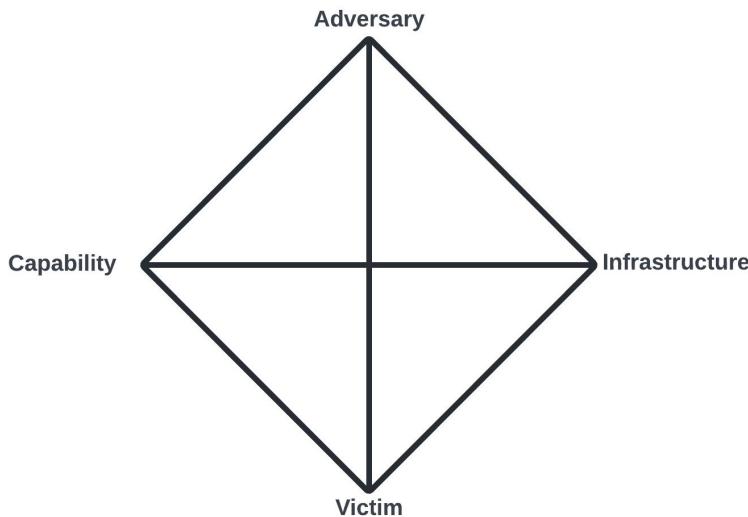
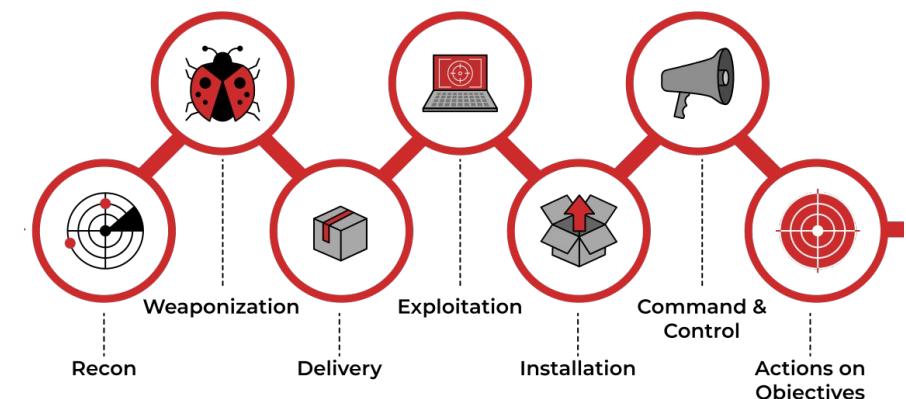
# Why do they look the way they do?

- Tree Structure
- Nodes & Leaves
- Relationships





# A decade of CTI taxonomies and frameworks



**MITRE**  
**ATT&CK**™

<https://apps.dtic.mil/sti/tr/pdf/ADA586960.pdf>

2011

2013

2014

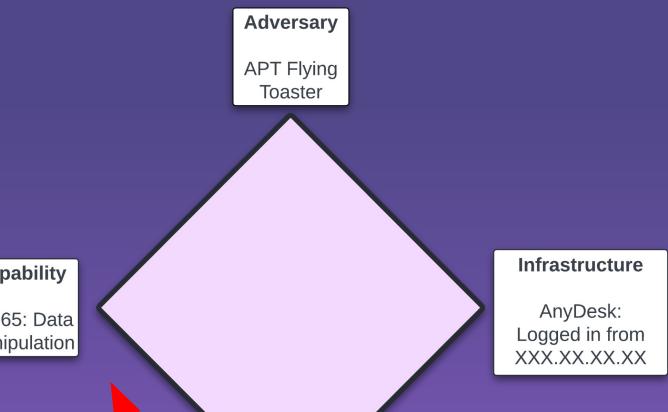
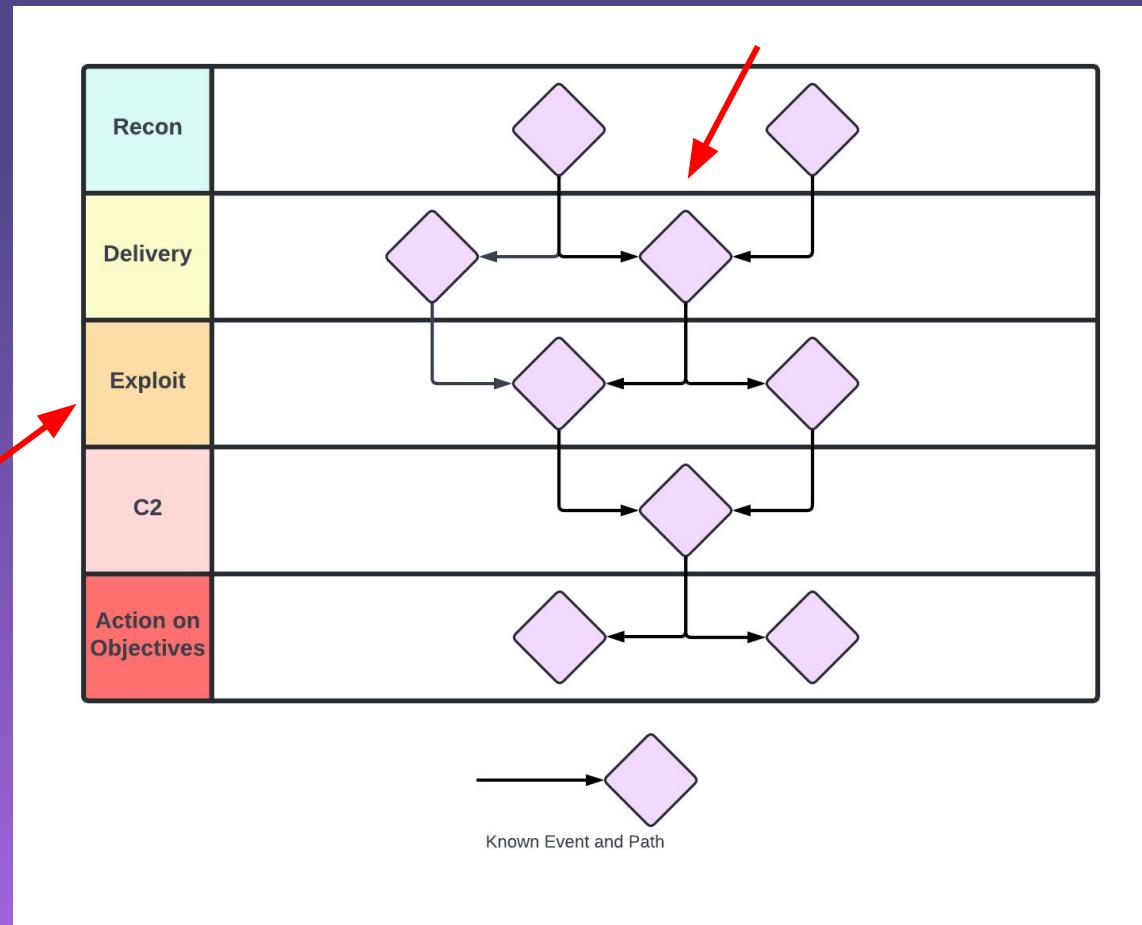


# Combining everything conceptually

**Diamond Model:**  
Structured documentation of attacker procedures  
and activity threading



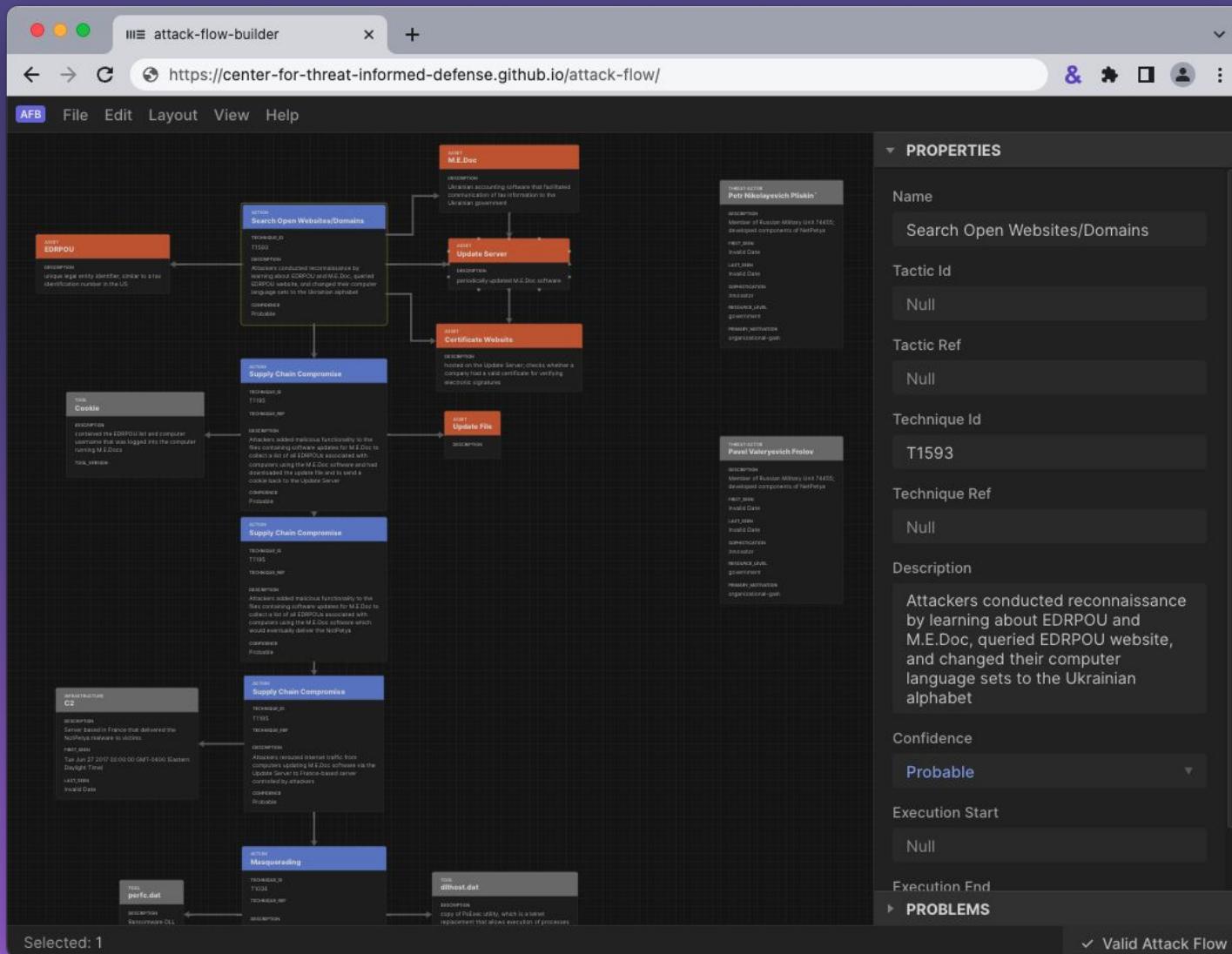
Kill Chain: Truncated  
attacker sequence



**MITRE ATT&CK:**  
Standardized tactics &  
techniques



# Combining everything practically

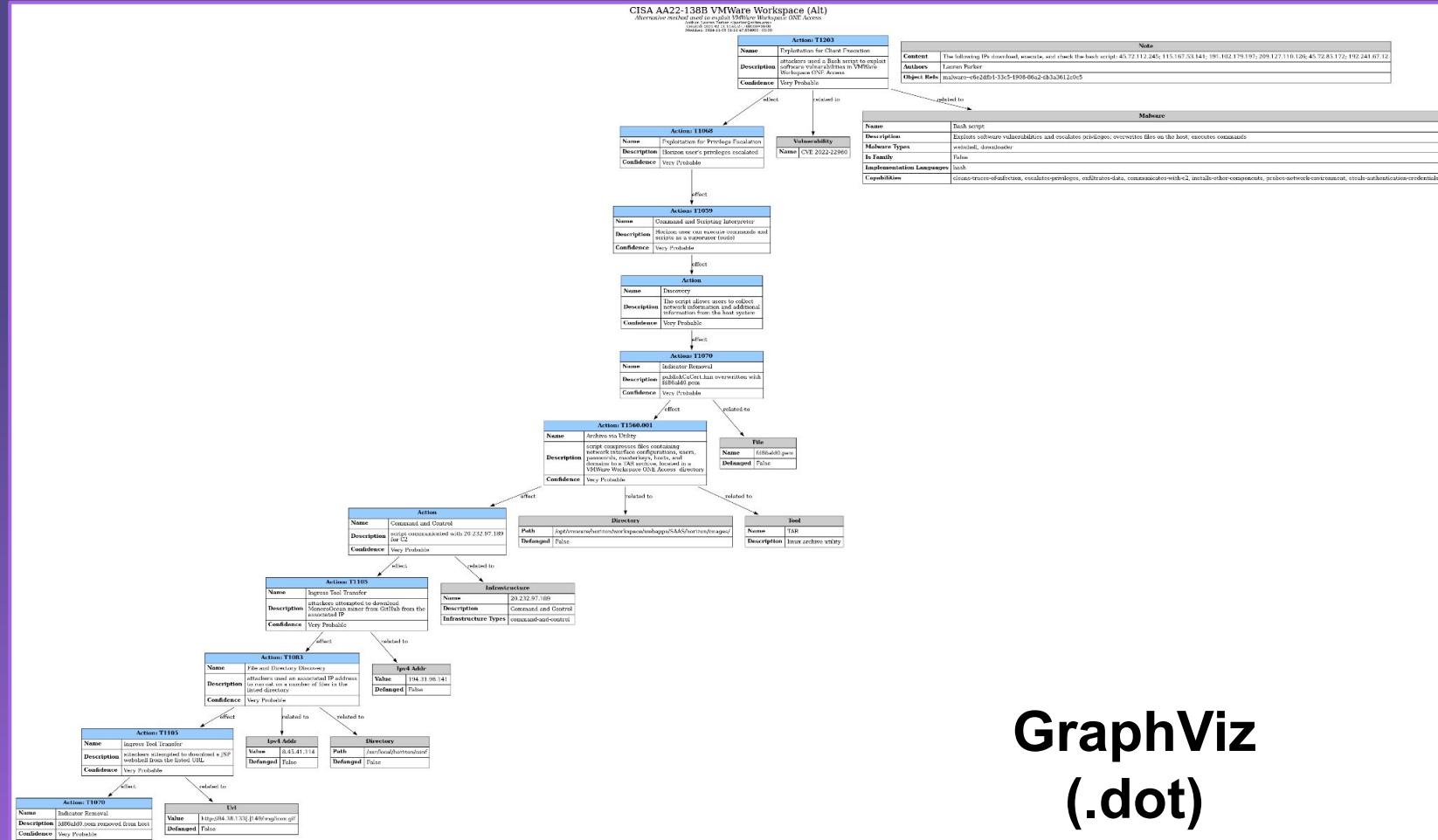


**Attack Flow**  
**Center for Threat**  
**Informed Defense**  
(direct link to builder)

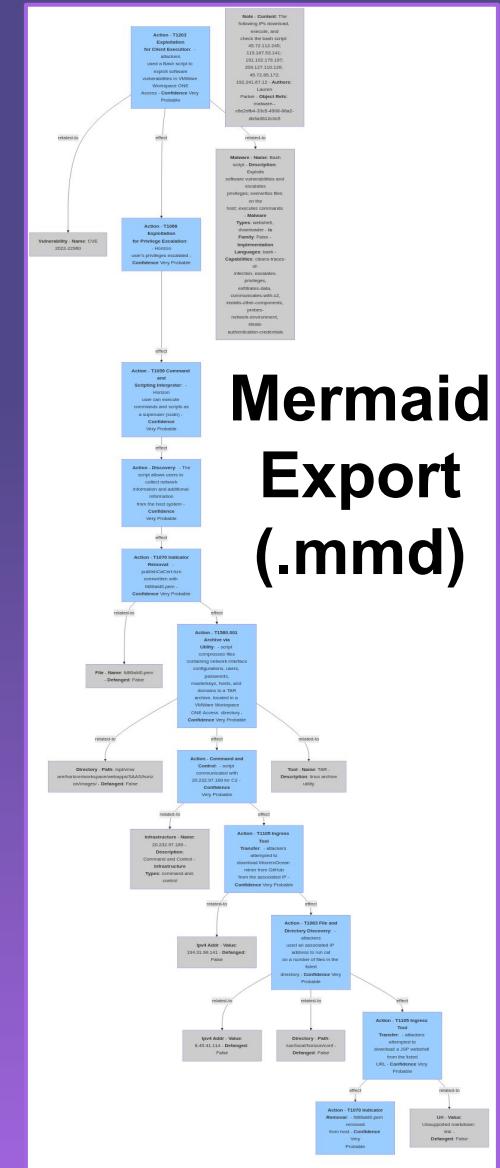




# Exporting into ‘official’ Attack Tree format



## GraphViz (.dot)



Everything JSON, making integration easier

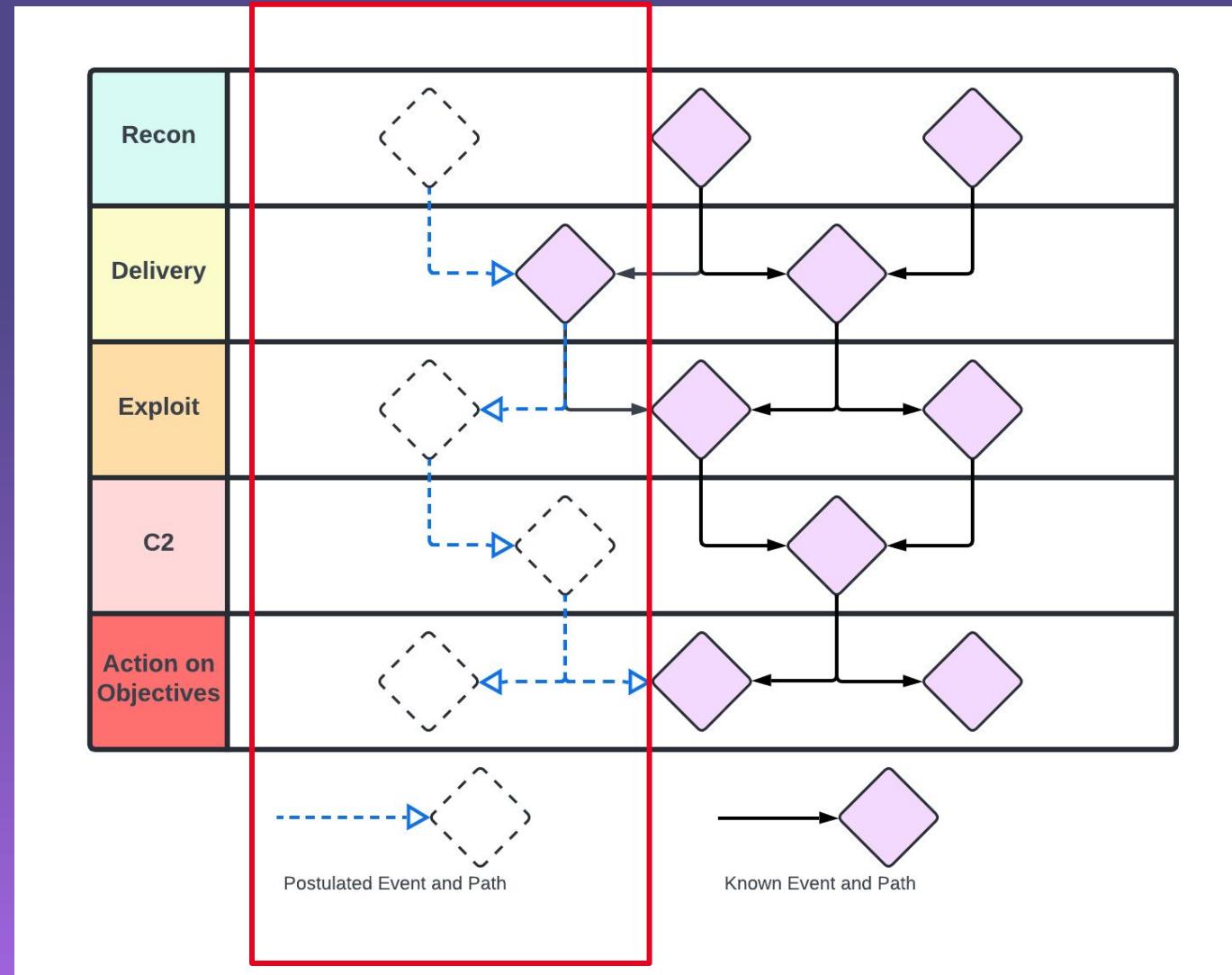
# Prioritizing Defensive Courses of Actions



# 'Postulating' TTPs

**Known  
Unknowns**

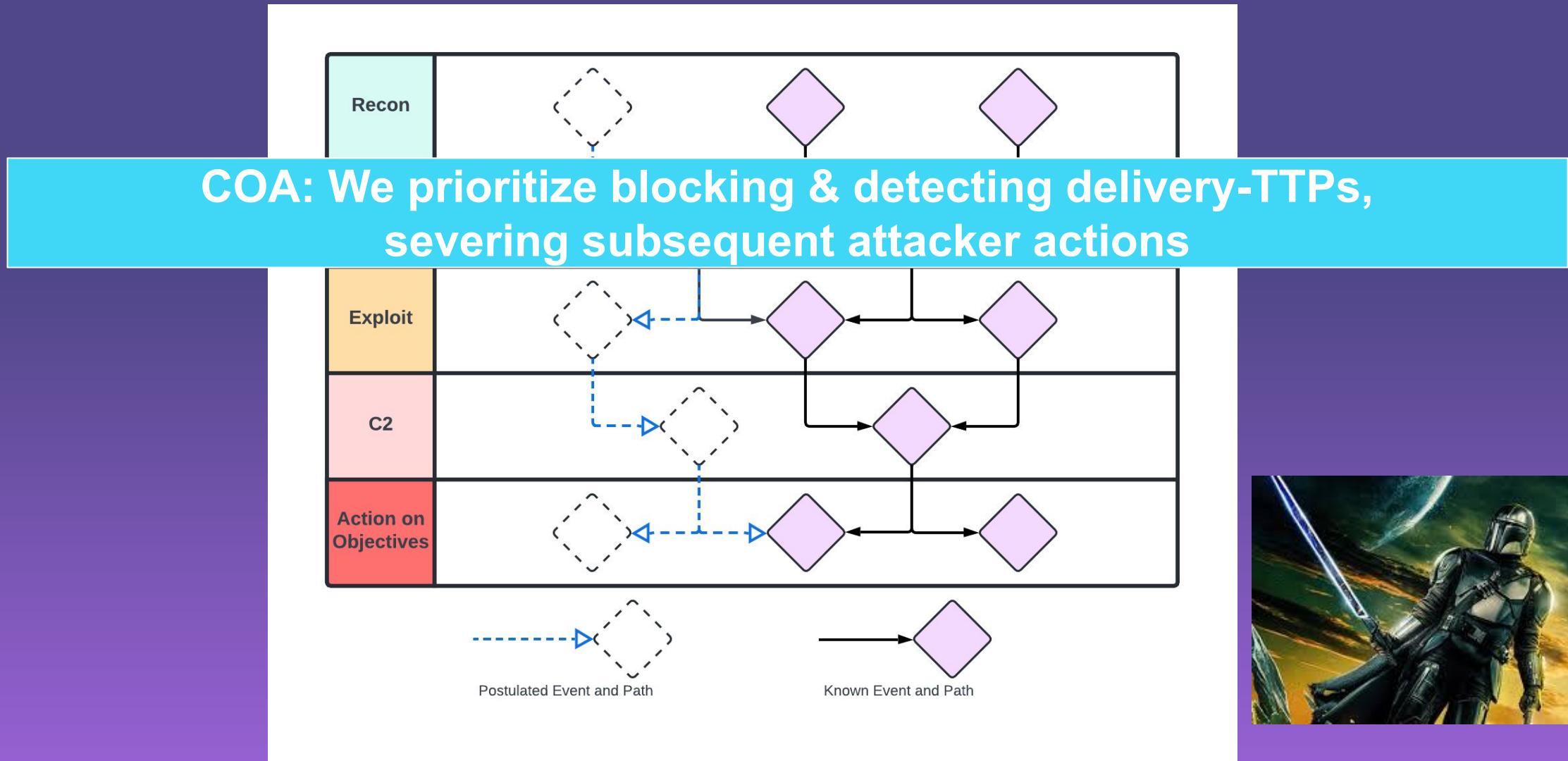
**Bonus:  
Testing for  
Unknown  
Unknown**



**Known  
Knowns**



# Conscious decision-making on ‘cutting ties’





# Prioritization through actionability

Source:  
<https://top-attack-techniques.mitre-enuity.org/>



Frequency of which an attacker uses a specific ATT&CK technique **over time**

Specific technique where many other techniques **converge or diverge**

Opportunity for defender to **detect or mitigate** against ATT&CK technique

Prevalence



Choke Point



Actionability



**Significant (Top) Techniques**



# This is not the Excel file you are looking for

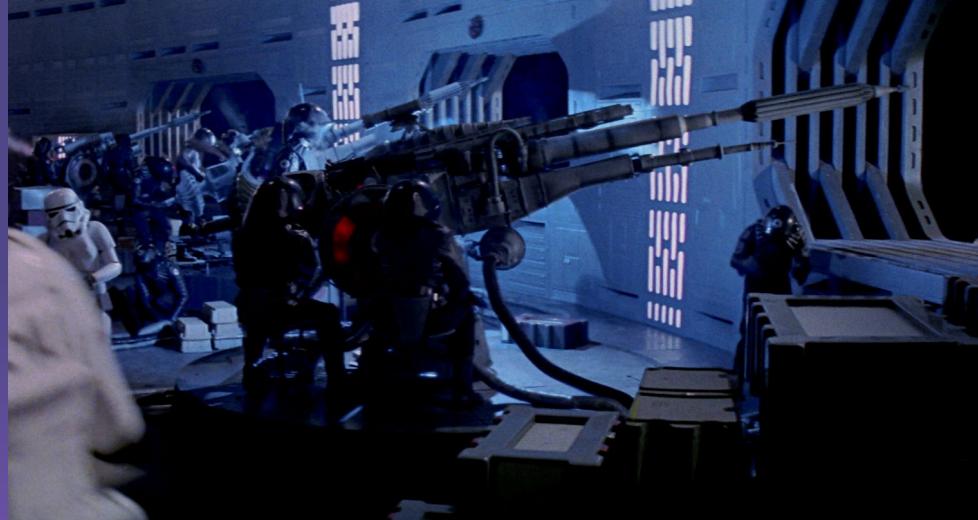
Technique (ID)	Technique (Name)	Num. TID	Num. TID After	Num. CAR	Num. Sigma	Num. ES SIEM	Num. Splunk	Num. CIS Controls	Num. 800-53 (r5)
T1053	Scheduled Task/Job	7	5	0	11	19	28	10	15
T1059	Command and Scripting Interpreter	10	15	1	51	64	57	22	24
T1562	Impair Defenses	1	1	3	74	39	45	8	16
T1055	Process Injection	3	6	0	23	13	26	9	12
T1036	Masquerading	1	1	1	27	16	27	7	12
T1218	Signed Binary Proxy Execution	1	1	0	94	18	70	14	18
T1574	Hijack Execution Flow	4	3	1	22	1	4	17	19
T1047	Windows Management Instrumentation	3	12	3	40	5	14	7	18
T1543	Create or Modify System Process	2	2	0	9	28	16	12	21
T1112	Modify Registry	1	1	8	62	5	25	1	2
T1021	Remote Services	4	5	1	3	34	24	7	12
T1105	Ingress Tool Transfer	5	3	4	47	9	23	2	8
T1204	User Execution	4	4	0	8	7	15	10	13
T1027	Obfuscated Files or Information	2	1	0	83	7	8	5	6
T1003	OS Credential Dumping	1	5	0	23	34	36	19	22
T1078	Valid Accounts	6	5	0	42	40	51	11	23

Source: <https://top-attack-techniques.mitre-engenuity.org/>





# Stakeholder and business operations engagement



## Defender Considerations



## Business Operation Considerations

Will applying detection or preventative course of actions disrupt business operations?

# What Does a Practical Attack Tree Example Look Like?



...  
Sometimes you have a lot of time,  
sometimes you don't



**Preliminary  
Assessment**



**Deliberate  
Assessment**



**In-depth  
Assessment**



•••

# Start with orientation

**What do we think  
we know about this  
threat**

**What do we think  
we know about  
ourselves**

**What do we think  
we don't know  
about this threat**

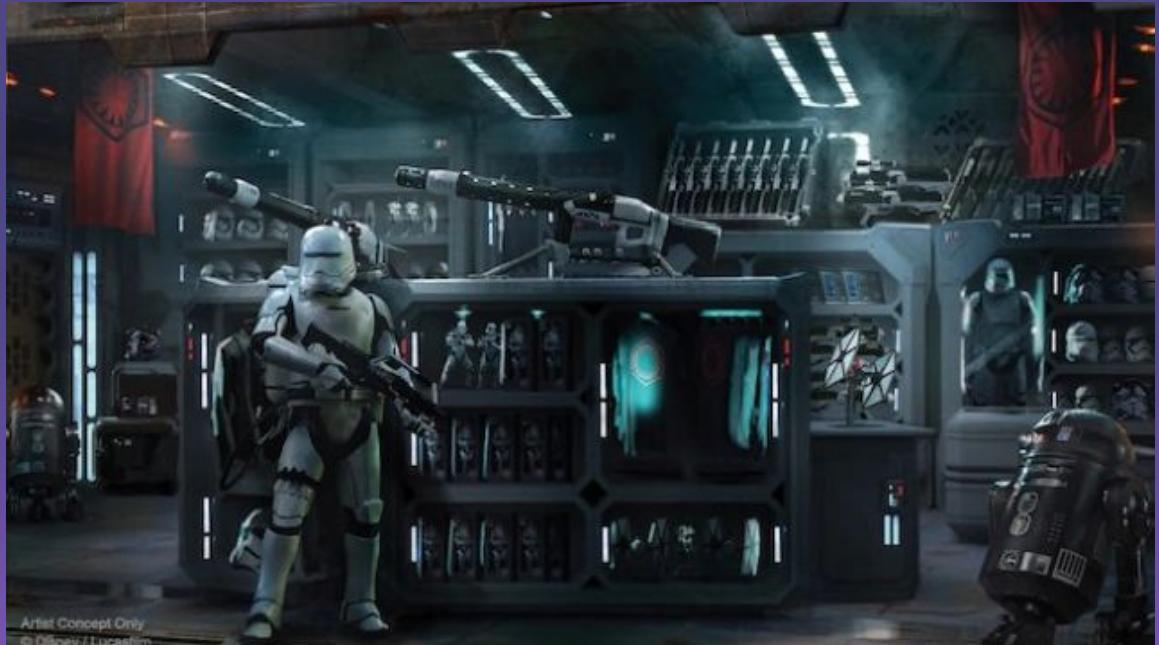
**What do we think  
we don't know  
about ourselves**



•••

# Where do you create the Attack Tree?

- Whiteboard or physical paper
- Attack Flow
- Any charting app (LucidChart, Visio, Draw.IO)





# Rough TTP mapping to establish graph

Case Studies

ASD's ACSC are sharing two anonymized investigative reports to provide awareness of how the actors employ their tools and tradecraft.

## Case Study 1

This report has been anonymized to enable wider dissemination. The impacted organization is hereafter referred to as "the organization." Some specific details have been removed to protect the identity of the victim and incident response methods of ASD's ACSC.

### Executive Summary

This report details the findings of the ASD's ACSC investigation into the successful compromise of the organization's network between July and September 2022. This investigative report was provided to the organization to summarize observed malicious activity and frame remediation recommendations. The findings indicate the compromise was undertaken by APT40.

In mid-August, the ASD's ACSC notified the organization of malicious interactions with their network from a likely compromised device being used by the group in late August and, with the organization's consent, the ASD's ACSC deployed host-based sensors to likely affected hosts on the organization's network. These sensors allowed ASD's ACSC incident response analysts to undertake a thorough digital forensics investigation. Using available sensor data, the ASD's ACSC analysts successfully mapped the group's activity and created a detailed timeline of observed events.

From July to August, key actor activity observed by the ASD's ACSC included:

- Host enumeration, which enables an actor to build their own map of the network;
- Web shell use, giving the actor an initial foothold on the network and a capability to execute commands; and
- Deployment of other tooling leveraged by the actor for malicious purposes.

The investigation uncovered evidence of large amounts of sensitive data being accessed and evidence that the actors moved laterally through the network [T1021\_002]. Much of the compromise was facilitated by the group's establishment of multiple access vectors into the network, the network having a flat structure, and the use of insecure internally developed software that could be used to arbitrarily upload files. Exfiltrated data included privileged authentication credentials that enabled the group to log in, as well as network information that would allow the actors to regain unauthorized access if the original access vector was blocked. No additional malicious tooling was discovered beyond those on the initially exploited machine; however, a group's access to legitimate and privileged credentials would negate the need for additional tooling. Findings from the investigation indicate the organization was likely deliberately targeted by APT40, as opposed to falling victim opportunistically to a publicly known vulnerability.

Source:  
<https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-190a>





# Continue adding research & extend graph

The screenshot shows a software interface for managing attack flows. On the left, a large blue box displays the current action: "Search Victim-Owned Websites". Below this, the Tactic ID is listed as TA0043 and the Technique ID as T1594. A "DESCRIPTION" section provides a detailed explanation of the action's purpose. At the bottom, the confidence level is noted as "Certain". On the right side of the interface, there are two panels: "PROPERTIES" and "PROBLEMS". The "PROPERTIES" panel contains fields for Name (APT 40 Case Study), Description (Example Attack Flow), Author (Sherm), Scope (Incident), and External References. The "PROBLEMS" panel is currently empty. The bottom status bar indicates "Selected: 0" and "Valid Attack Flow".

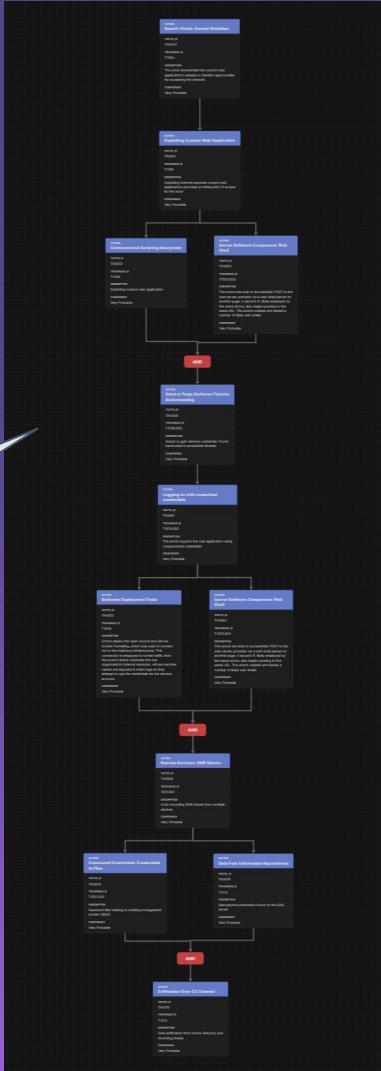
Source:  
<https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-190a>





# It doesn't take long before it is useful

Time Taken:  
~ 30 minutes

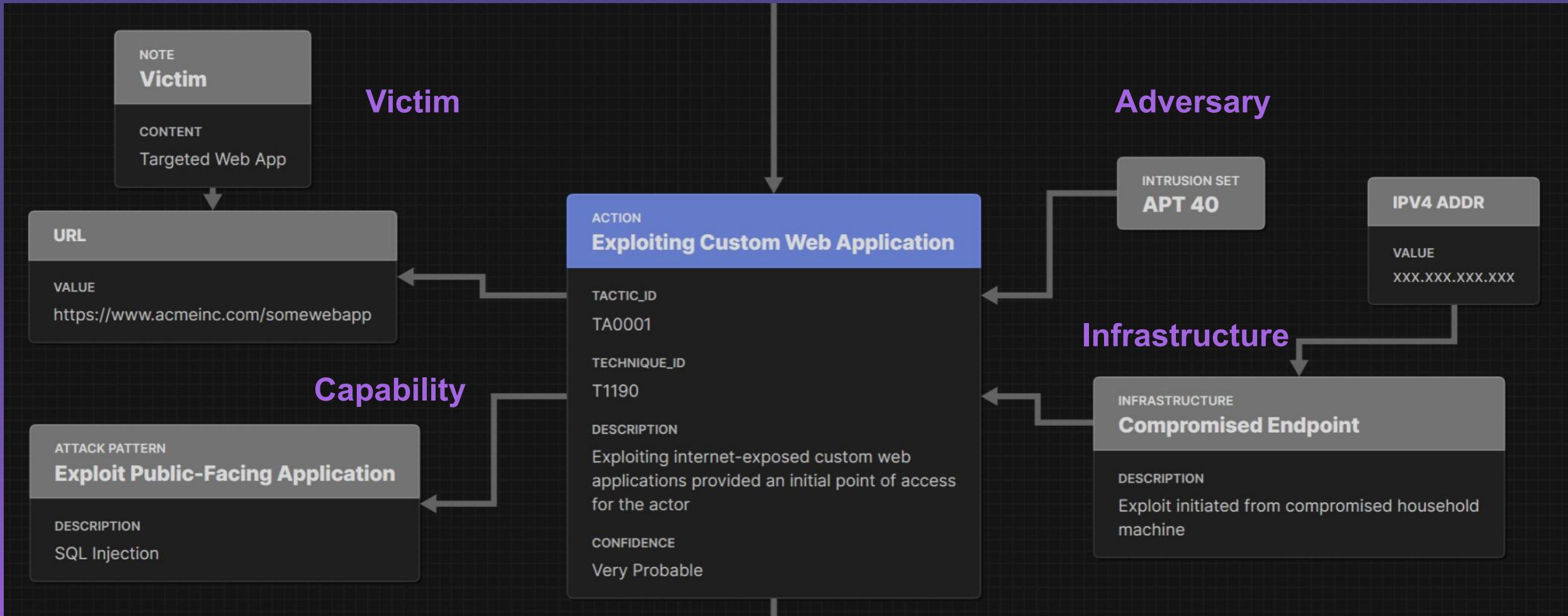


Source:  
<https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-190a>



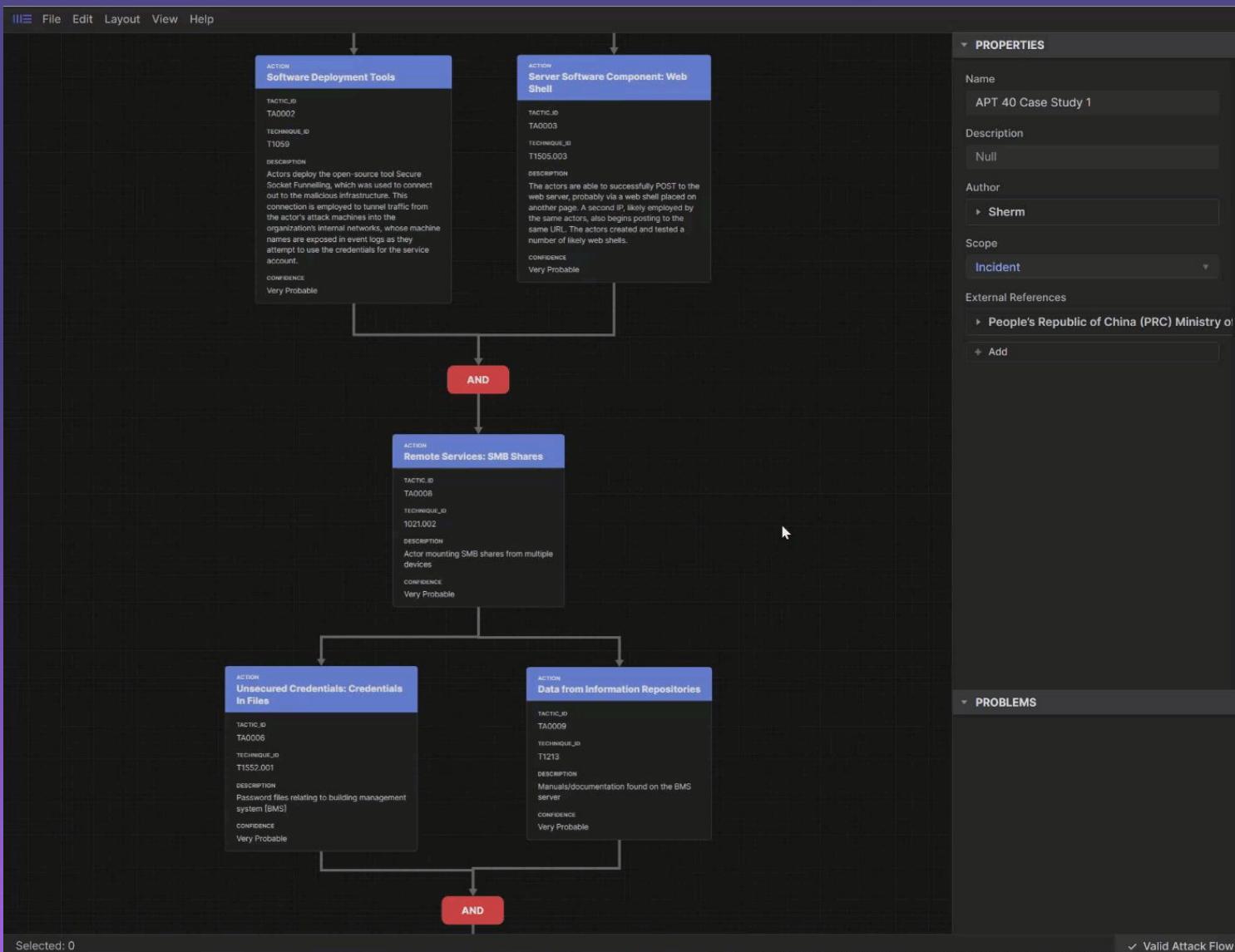


# Dive deeper into specific components





# Postulation & adding events



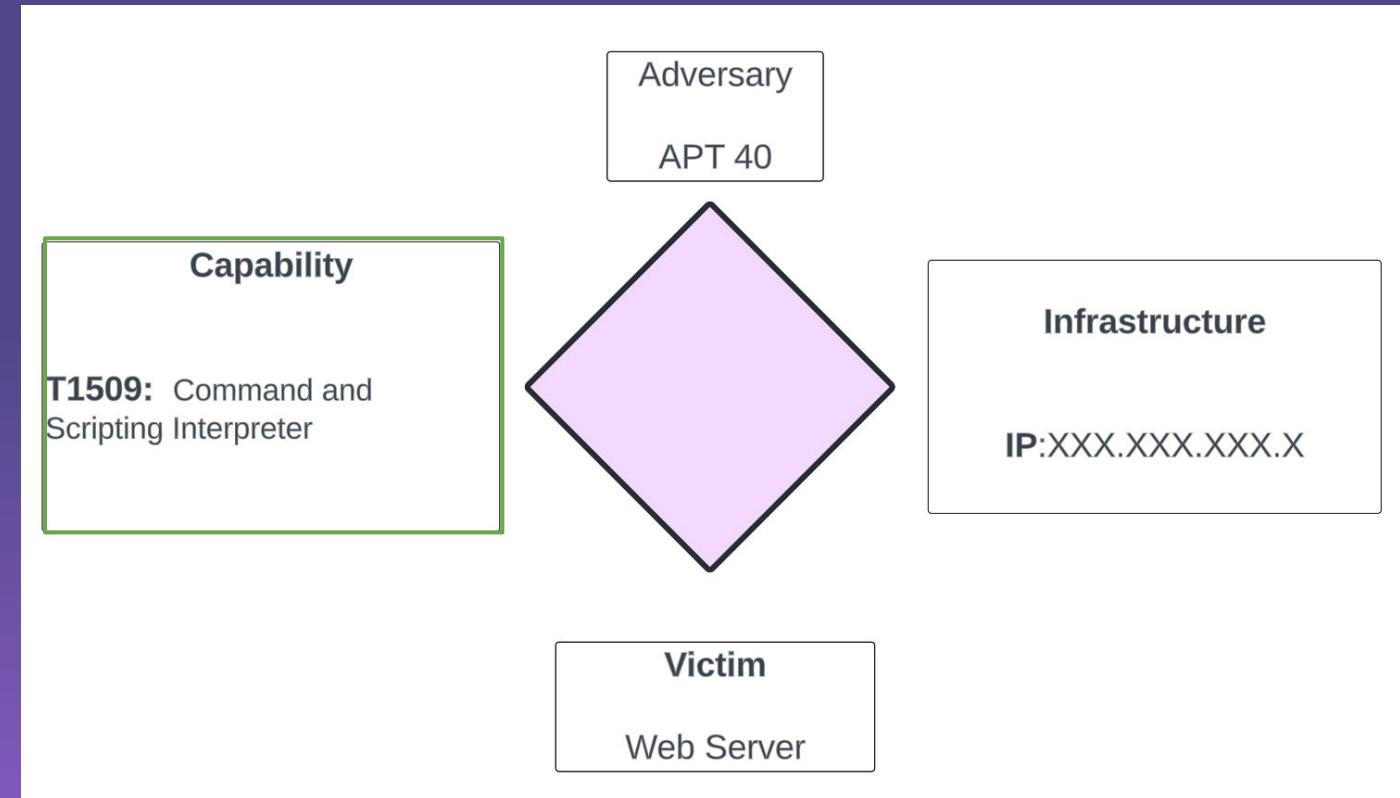


•••

# Prioritization assessment

↓

ACTION
<b>Command and Scripting Interpreter</b>
TACTIC_ID
TA0002
TECHNIQUE_ID
T1059
DESCRIPTION
Command execution through the web shell
CONFIDENCE
Very Probable





# Prevalence & choke points

Execution (TA0002)	
Windows Management Instrumentation [T1047]	Command and Scripting Interpreter: Python [T1059.006]
Scheduled Task/Job: At [T1053.002]	Command and Scripting Interpreter: JavaScript [T1059.007]
Scheduled Task/Job: Scheduled Task [T1053.005]	Native API [T1106]
Command and Scripting Interpreter [T1059]	Inter-Process Communication [T1559]
Command and Scripting Interpreter: Windows Command Shell [T1059.003]	System Services: Service Execution [T1569.002]
Command and Scripting Interpreter: PowerShell [T1059.001]	Exploitation for Client Execution [T1203]
Command and Scripting Interpreter: Visual Basic [T1059.005]	User Execution: Malicious File [T1204.002]
Command and Scripting Interpreter: Unix Shell [T1059.004]	Command and Scripting Interpreter: Apple Script [T1059.002]
Scheduled Task/Job: Cron [T1053.003]	Software Deployment Tools [T1072]

Super prevalent example

Technique (Name)	Num. TID Before	Num. TID After	Choke Point	Before	After Util	After Util
Scheduled Task/Job	/	5	0.6	0.7	0.7	0.5
Command and Scripting Interpreter	10	15	1	1	1	1.5
Impair Defenses	1	1	0.1	0.1	0.1	0.1
Process Injection	3	6	0.4	0.3	0.3	0.6
Masquerading	1	1	0.1			
Signed Binary Proxy Execution	1	1				
Hijack Execution Flow	4	3				

Force choke target



# Actionability assessment

Amount of  
readily available  
Splunk content



## Content by Tag

Splunk Enterprise	1581
Splunk Enterprise Security	172
Defense Evasion	991
Persistence	516
Execution	289
Lateral Movement	86
Splunk Behavioral Analytics	74
Disable or Modify Tools	71
Resource Development	67
Modify Registry	61
Brute Force	43
Account Discovery	41
User Execution	39
Splunk Endpoint	73
Initial Access	325
Discovery	266
Impact	85
Impair Defenses	97
Command And Control	83
System Binary Proxy Execution	73
Exploit Public-Facing Application	68
Valid Accounts	62
Cloud Accounts	59
Abuse Elevation Control Mechanism	57
PowerShell	42
Exfiltration	41
OS Credential Dumping	39
Phishing	39
Spearphishing Attachment	36
External Remote Services	34

## Command and Scripting Interpreter

### Collection

73

69



## T1059 COMMAND AND SCRIPTING INTERPRETER MAPPINGS

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of Unix Shell while Windows installations include the Windows Command Shell and PowerShell.

There are also cross-platform interpreters such as Python, as well as those commonly associated with client applications such as JavaScript and Visual Basic.

Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in Initial Access payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various Remote Services in order to achieve remote Execution.(Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

[View in MITRE ATT&CK®](#)

## MAPPINGS

ATT&CK Version 14.1 ATT&CK Domain Enterprise Change Versions

Capability ID	Capability Description	Mapping Type	ATT&CK ID	ATT&CK Name
AC-17	Remote Access	Protects	T1059	Command and Scripting Interpreter
AC-02	Account Management	Protects	T1059	Command and Scripting Interpreter
AC-03	Access Enforcement	Protects	T1059	Command and Scripting Interpreter
AC-05	Separation of Duties			
AC-06	Least Privilege			
CA-07	Continuous Monitoring			
CM-05	Access Restrictions for Change			

Capability ID	Capability Description
AC-17	Remote Access
AC-02	Account Management
AC-03	Access Enforcement
AC-05	Separation of Duties
AC-06	Least Privilege
CA-07	Continuous Monitoring

NIST 800-53 Controls



# Defensive capability & business ops. considerations

Volt Typhoon uses at least the following LOTL tools and commands for system information, network service, group, and user discovery techniques:

- cmd
- certutil
- dnscmd
- ldifde
- makecab
- net user/group/use
- netsh
- nltest
- netstat
- ntdsutil
- ping
- PowerShell
- quser
- reg query/reg save
- systeminfo
- tasklist
- wevtutil
- whoami
- wmic
- xcopy

## Example questions:

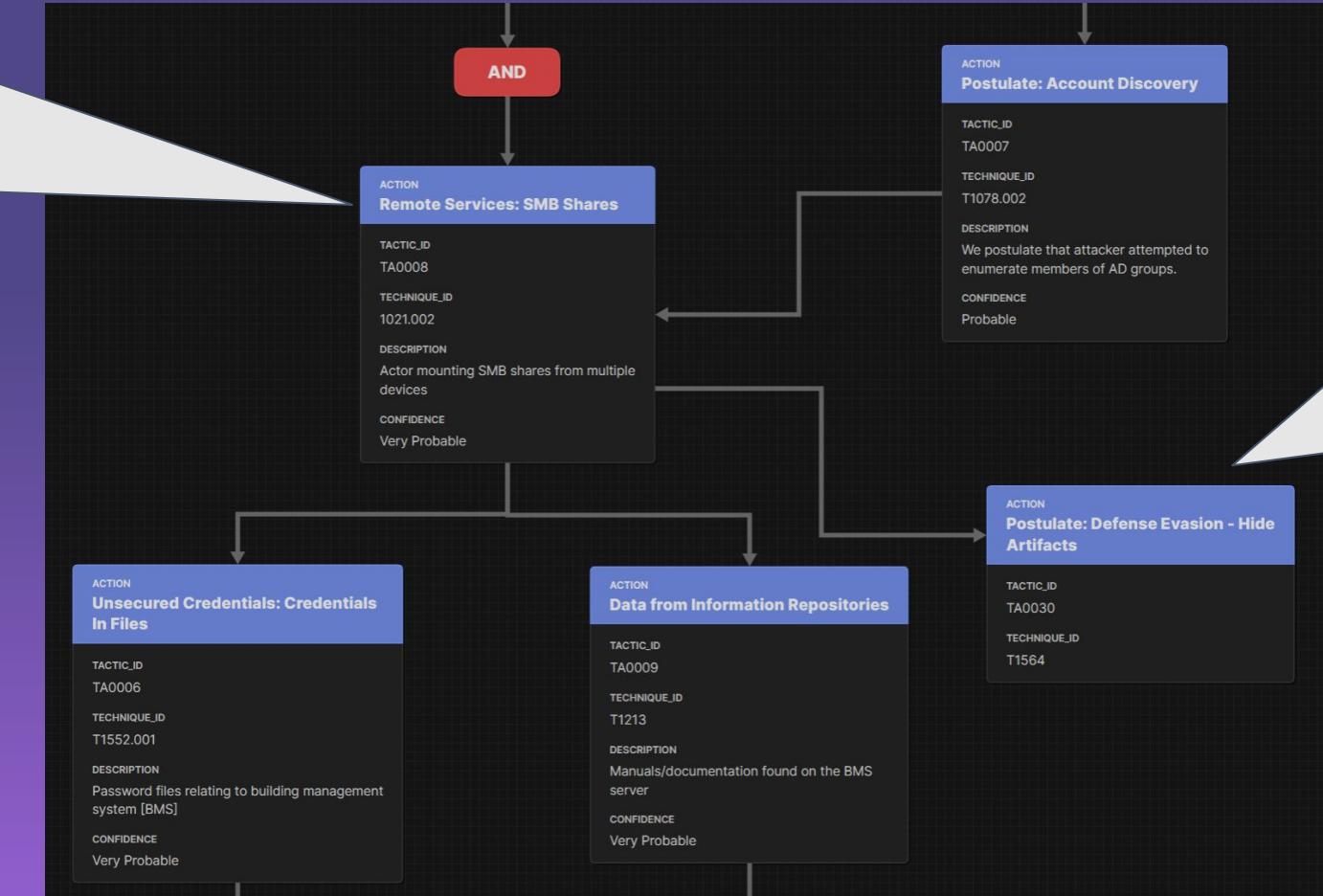
- How common is PowerShell usage in org?
- Will IT/Business Ops be mad if we limit PowerShell use?

Source: <https://research.splunk.com/tags/#external-remote-services> & <https://center-for-threat-informed-defense.github.io/mappings-explorer>



# Conscious prioritization

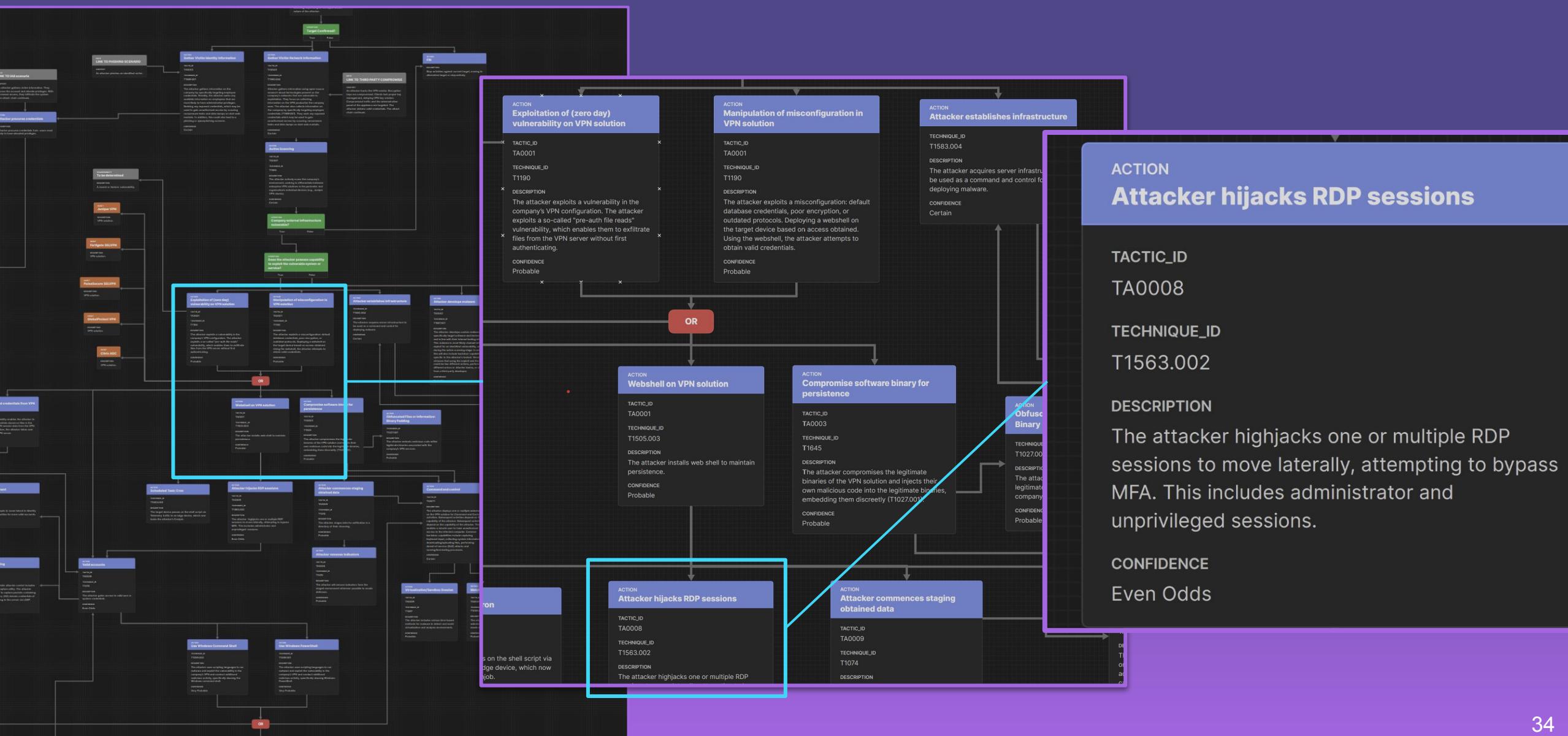
“We know exactly how to this element will be prevented”



“We don't know how defense evasion will play out in our scenario”

Where does that leave us?

# Which stakeholders benefits & how





# What Attack Trees are really about

...

**Threat  
Landscape  
& Surface**

**Attack  
Trees**

**Defensive  
Measures**

## Today:

- A mental model, evolving based on new innovations
- Investigate Attack Flow (Center for Threat Informed Defense)

## Tomorrow:

- Use Attack Trees in your next IR report, RT engagement or for supporting security investment decisions.

(direct link to Attack  
Flow builder)





# Find us via the following channels



## Sherman Chu

Threat-Informed Defense Advocate  
Warhammer Nerd  
CTI Lead at BlackRock

X: @aperturenoise  
LinkedIn: /shermanchu1



## Gert-Jan Bruggink

Cyber threat cartographer  
CTI Bob Ross  
Cyber weatherman  
ceo & founder Venation

X: @gertjanbruggink  
LinkedIn: /gertjanbruggink  
Newsletter: <https://venation.digital/newsletter>

# Here's the references:

Description	Link
Attack Flow Tool	<a href="https://center-for-threat-informed-defense.github.io/attack-flow/ui/">https://center-for-threat-informed-defense.github.io/attack-flow/ui/</a>
Attack Flow Build files used for the examples in this presentation	<a href="https://github.com/gertjanbruggink/templates/tree/master/Attack%20Trees">https://github.com/gertjanbruggink/templates/tree/master/Attack%20Trees</a>
Draw IO Attack Tree Template	<a href="https://github.com/gertjanbruggink/templates/tree/master/Attack%20Trees">https://github.com/gertjanbruggink/templates/tree/master/Attack%20Trees</a>
Repository of Attack Flow premade threat scenarios (paid):	<a href="https://venation.digital/scenario-intelligence">https://venation.digital/scenario-intelligence</a>
CTID Mappings	<a href="https://center-for-threat-informed-defense.github.io/mappings-explorer">https://center-for-threat-informed-defense.github.io/mappings-explorer</a>
Splunk tagging	<a href="https://research.splunk.com/tags/#external-remote-services">https://research.splunk.com/tags/#external-remote-services</a>
ME Top Techniques	<a href="https://top-attack-techniques.mitre-engenuity.org/">https://top-attack-techniques.mitre-engenuity.org/</a>
CISA advisory example	<a href="https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-190a">https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-190a</a>