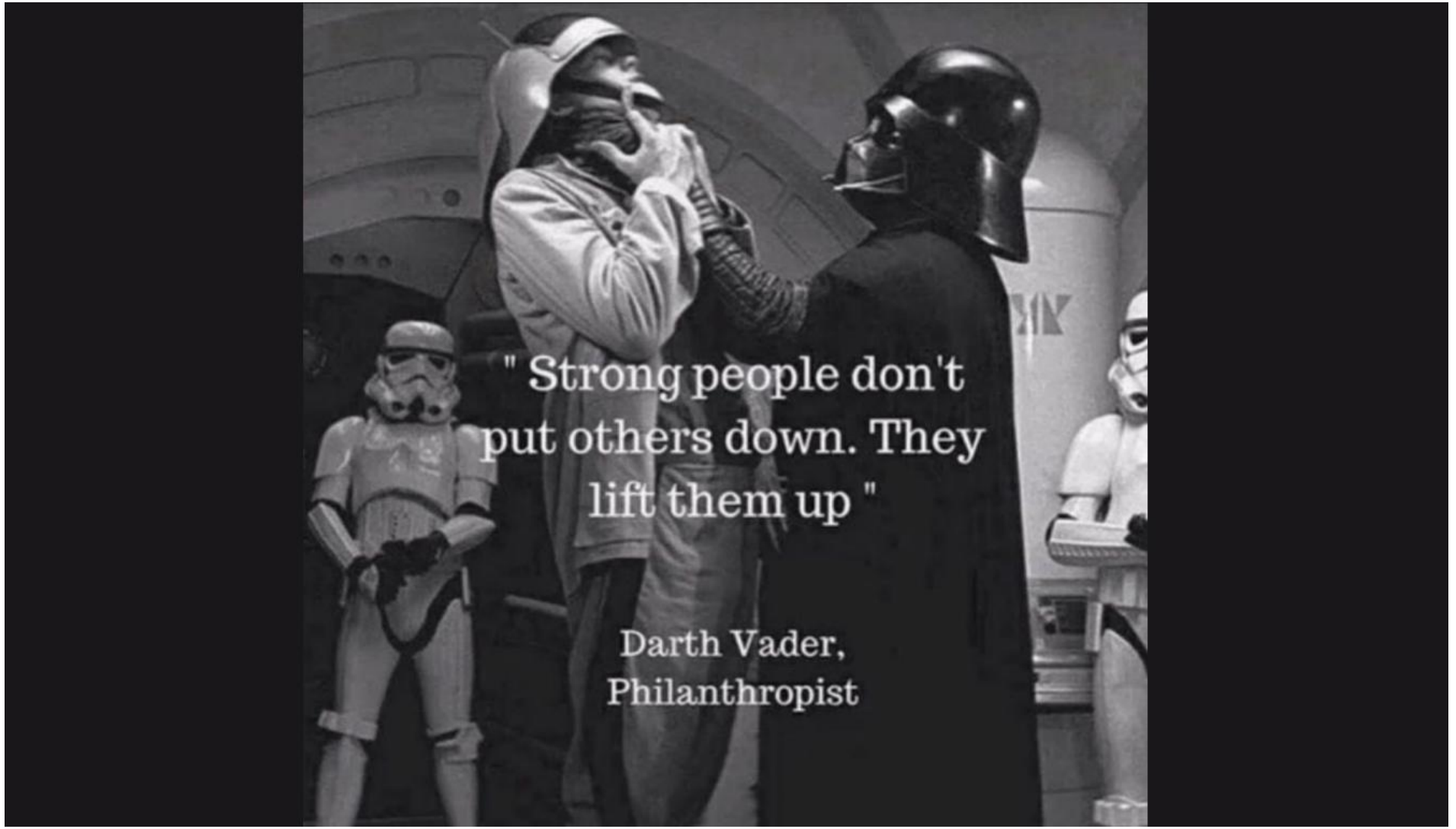
Decoding Cyber Threats

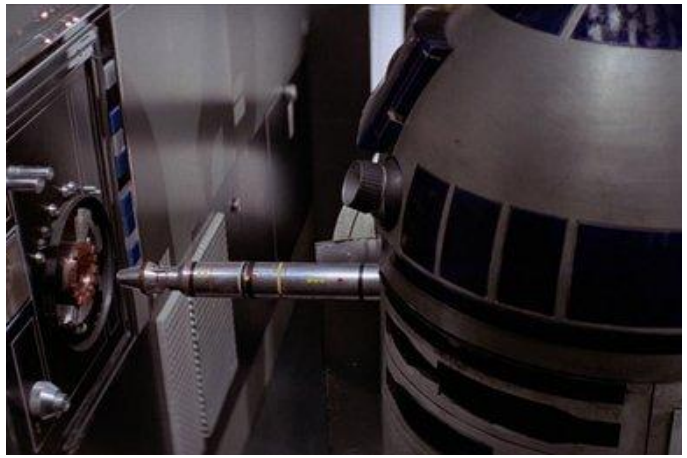
A Practical Guide to Using Attack Trees

Gert-Jan Bruggink | Sherman Chu

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

01

Why
Attack
Trees

02

How
Attack
Trees

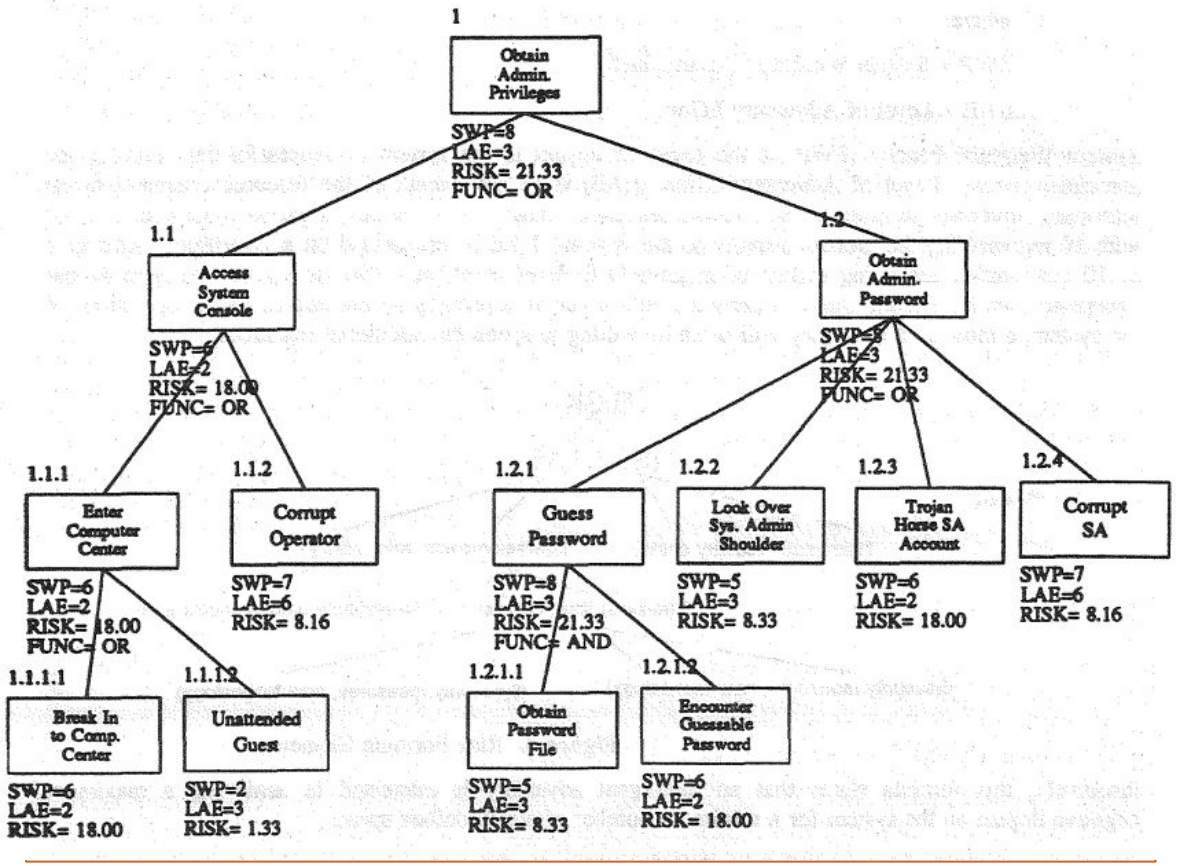
03

What
Attack
Trees

Why Attack Trees in the First Place

Why Were Attack Trees Created in the First Place?

- Visualize attack scenarios
- Threat modeling
- Decision making



Jonathan Weiss, 1982

A Little bit of History (We Love That Stuff)

1982
Conceptualized as threat trees by Jonathan Weiss, Bell laboratories

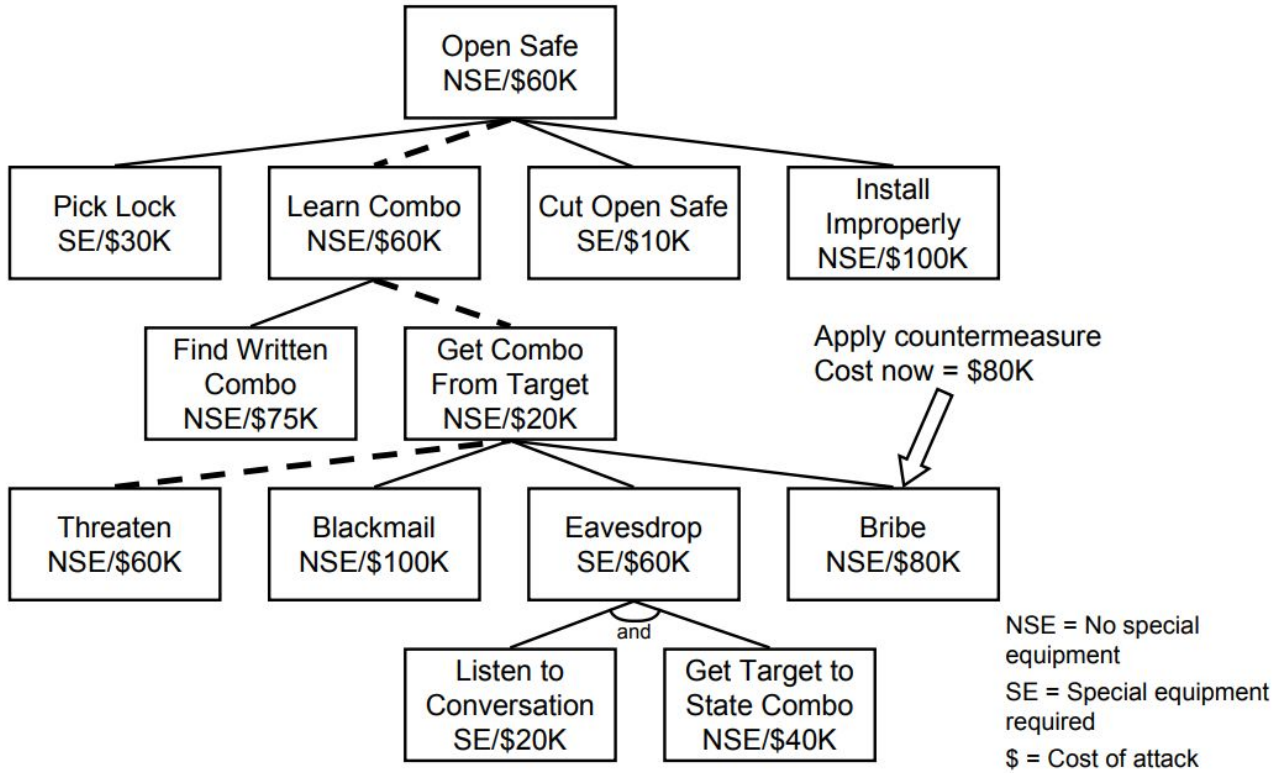
1999
Bruce Schneier publishes attack tree concepts

2013
Diamond Model of Intrusion incorporates attack tree attributes

2024
Two nerds at a CTI conference

Why do They Look the way They do?

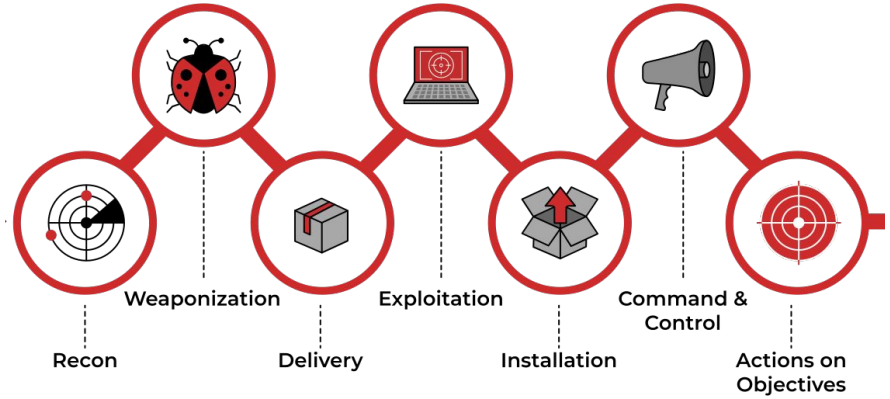
- Tree structure
- Nodes & leaves
- Relationships

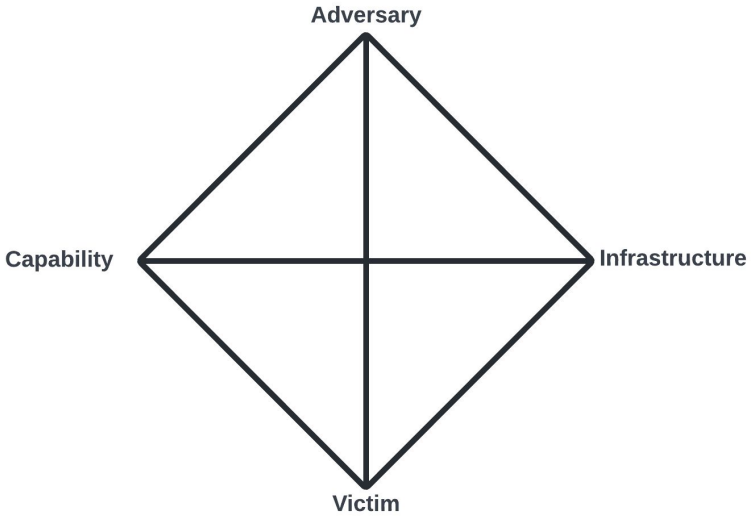


Bruce Schneier, 1995

Expanding Attack Trees Using Contemporary Cyber Threat Intelligence Practices

A Decade of CTI Taxonomies and Frameworks





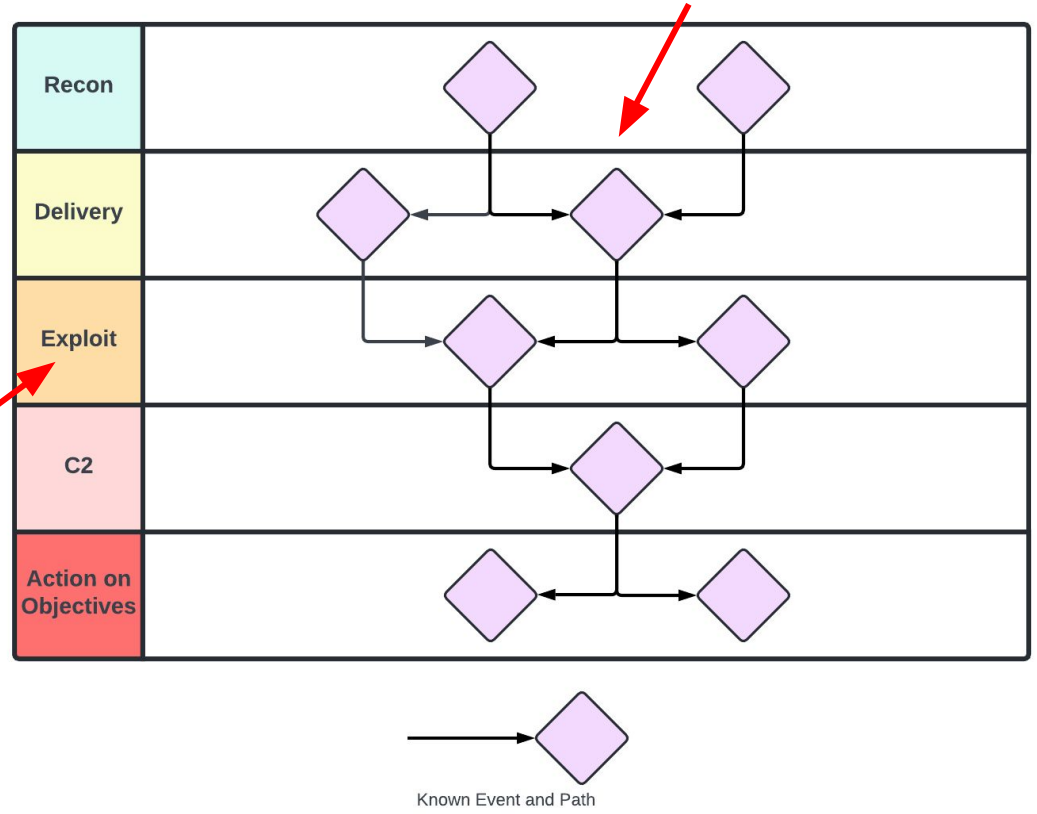
https://apps.dtic.mil/sti/tr/pdf/ADA586960.pdf

MITRE ATT&CK™

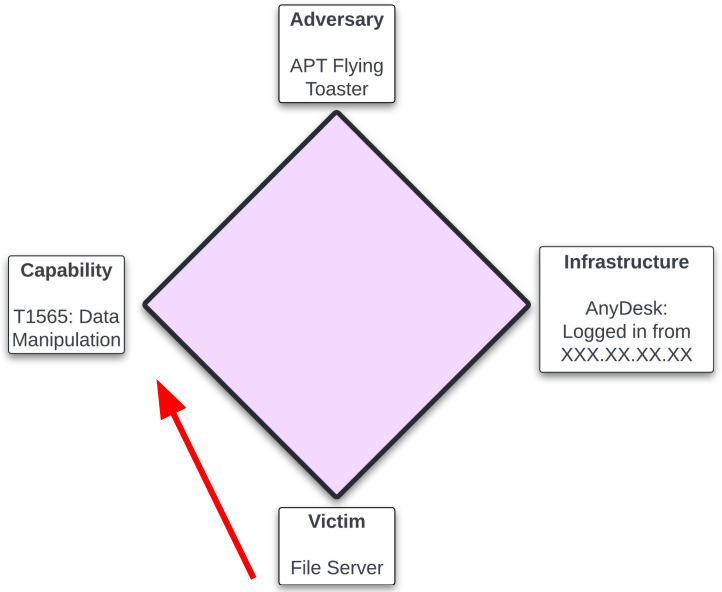
2011 **2013** **2014**

Combining it all

Diamond Model:
Structured documentation of attacker procedures and activity threading



Kill Chain: Truncated attacker sequence



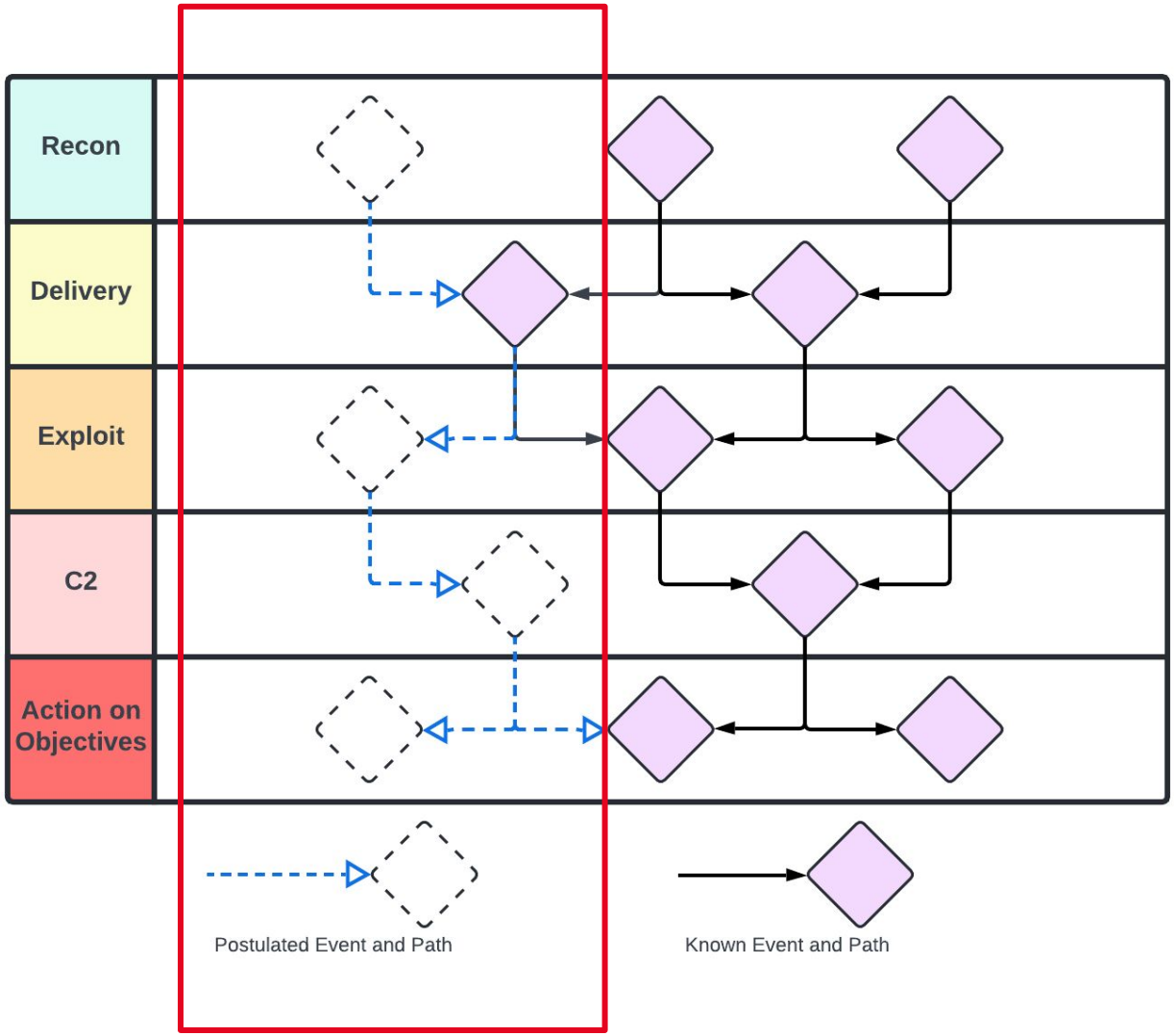
MITRE ATT&CK: Standardized tactics & techniques

How to leverage the essence: Prioritizing Defensive Courses of Actions

Adding Postulated TTPs

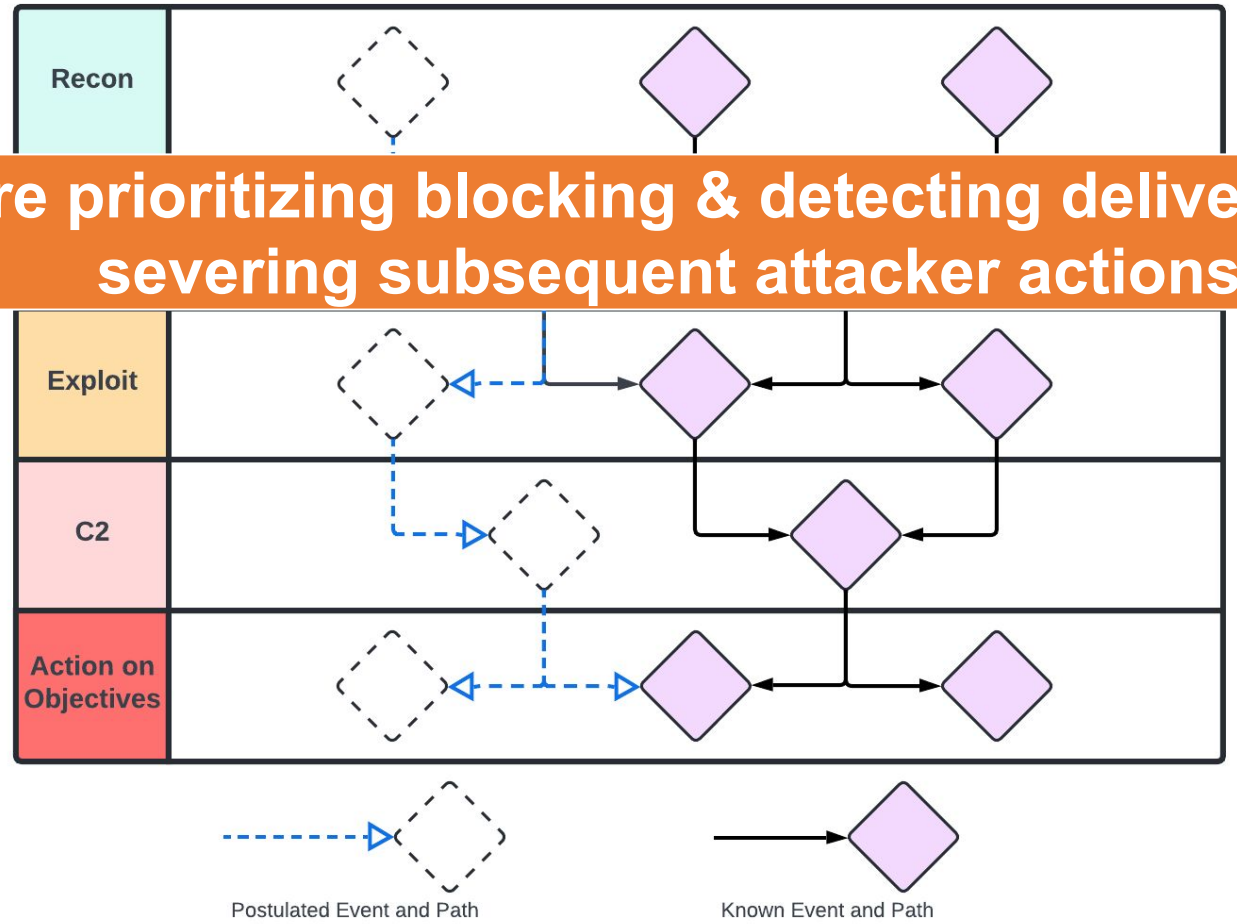
Known Unknowns

Bonus: Testing for Unknown Unknown



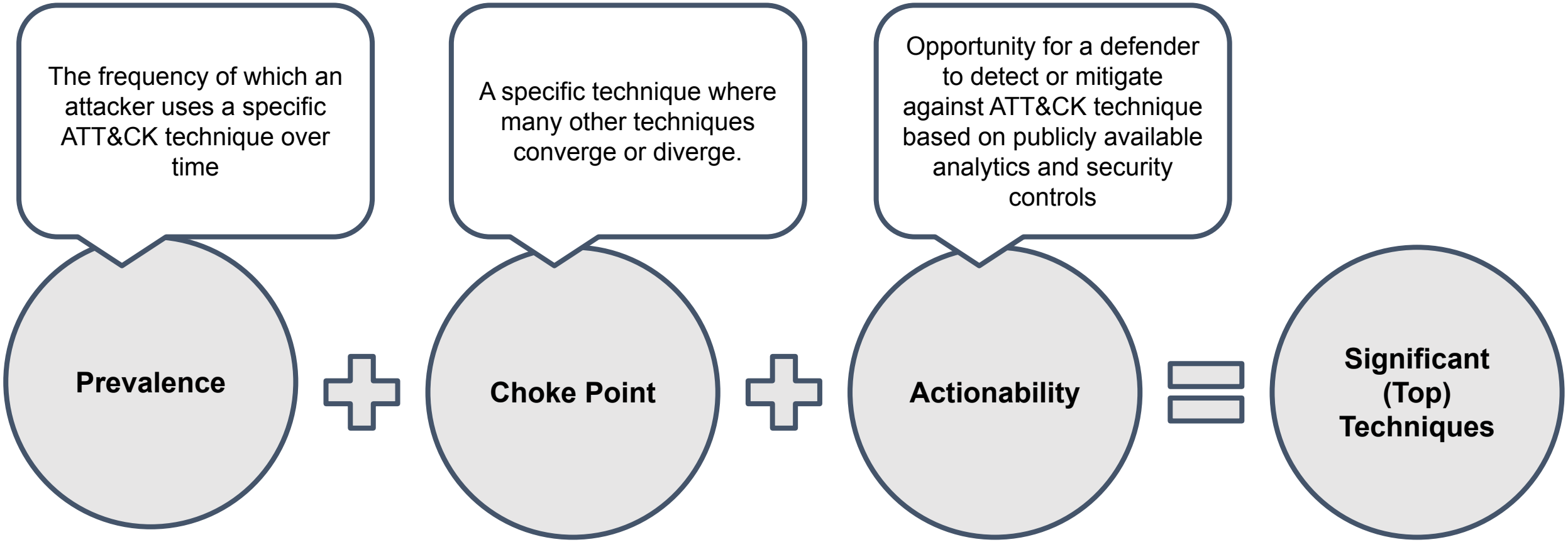
Known Knowns

Conscious decision making on cutting the ties



We are prioritizing blocking & detecting delivery-TTPs, severing subsequent attacker actions

Prioritization Through Actionability



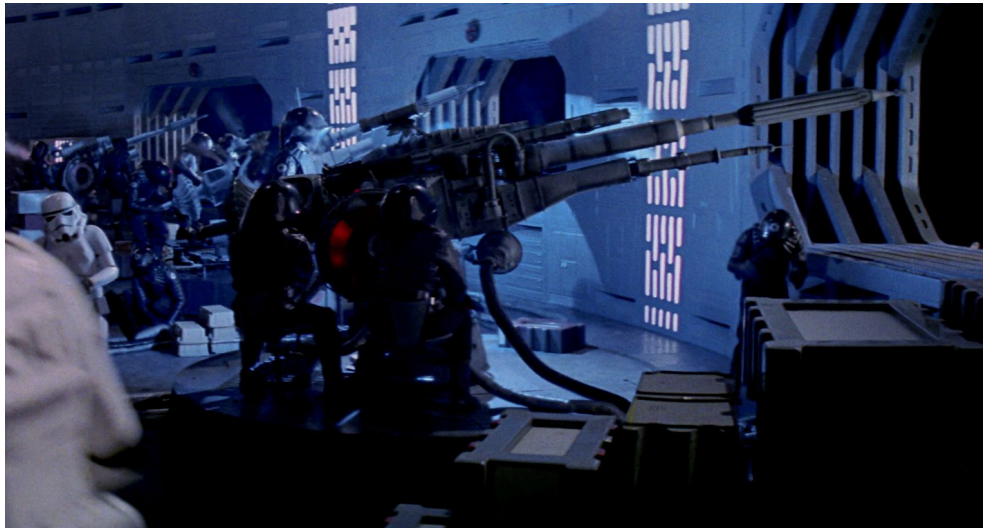
Source: https://top-attack-techniques.mitre-engenuity.org/

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?

An Event Occurs, Resulting in an Incident

Preliminary Assessment

Deliberate Assessment

In-depth Assessment

Preliminary	✅	Deliberate	✅	Indepth	✅

Orient Yourself

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

Preliminary	✅	Deliberate	✅	Indepth	✅

Where Do You Do This?

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

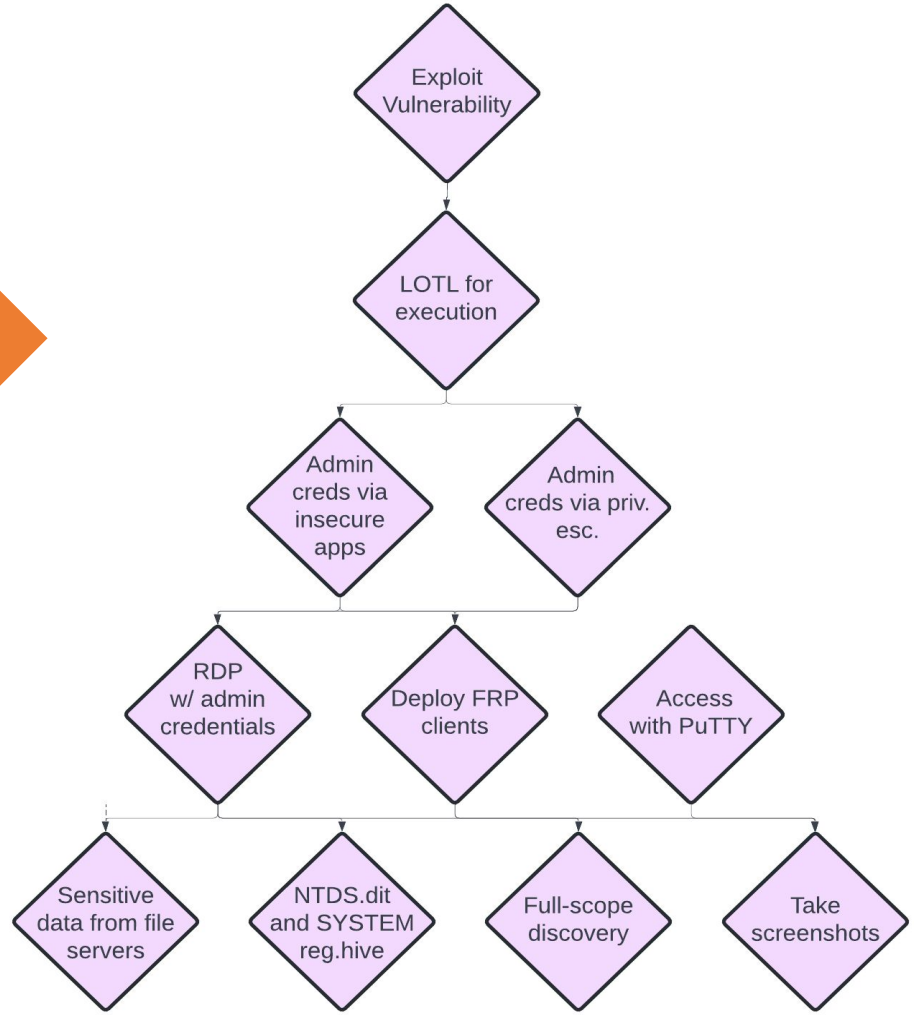
Preliminary	✅	Deliberate	✅	Indepth	✅

Rough TTP Mapping to Establish Attack Tree

1. **Volt Typhoon conducts extensive pre-compromise reconnaissance to learn about the target organization's network architecture and operational protocols.** This reconnaissance includes identifying network topologies, security measures, typical user behaviors, and key network and IT staff. The intelligence gathered by Volt Typhoon actors is likely leveraged to enhance their operational security. For example, in some instances, Volt Typhoon actors may have abstained from using compromised credentials outside of normal working hours to avoid triggering security alerts on abnormal account activities.
2. **Volt Typhoon typically gains initial access to the IT network by exploiting known or zero-day vulnerabilities in public-facing network** appliances (e.g., routers, virtual private networks [VPNs], and firewalls) and then connects to the victim's network via VPN for follow-on activities.
3. **Volt Typhoon aims to obtain administrator credentials within the network, often by exploiting privilege escalation vulnerabilities in the operating system or network services.** In some cases, Volt Typhoon has obtained credentials insecurely stored on a public-facing network appliance.
4. **Volt Typhoon uses valid administrator credentials to move laterally to domain controller (DC) and other devices** via remote access services suc Remote Desktop Protocol (RDP).
5. **Volt Typhoon conducts discovery in the victim's network, leveraging L binaries for stealth**. A key tactic includes using PowerShell to perform tar queries on Windows event logs, focusing on specific users and periods. Th queries facilitate the discreet extraction of security event logs into `.dat` f allowing Volt Typhoon actors to gather critical information while minimizi detection. This strategy, blending in-depth pre-compromise reconnaissan with meticulous post-exploitation intelligence collection, underscores the sophisticated and strategic approach to cyber operations.

Random publicly available report

~ 30 minutes

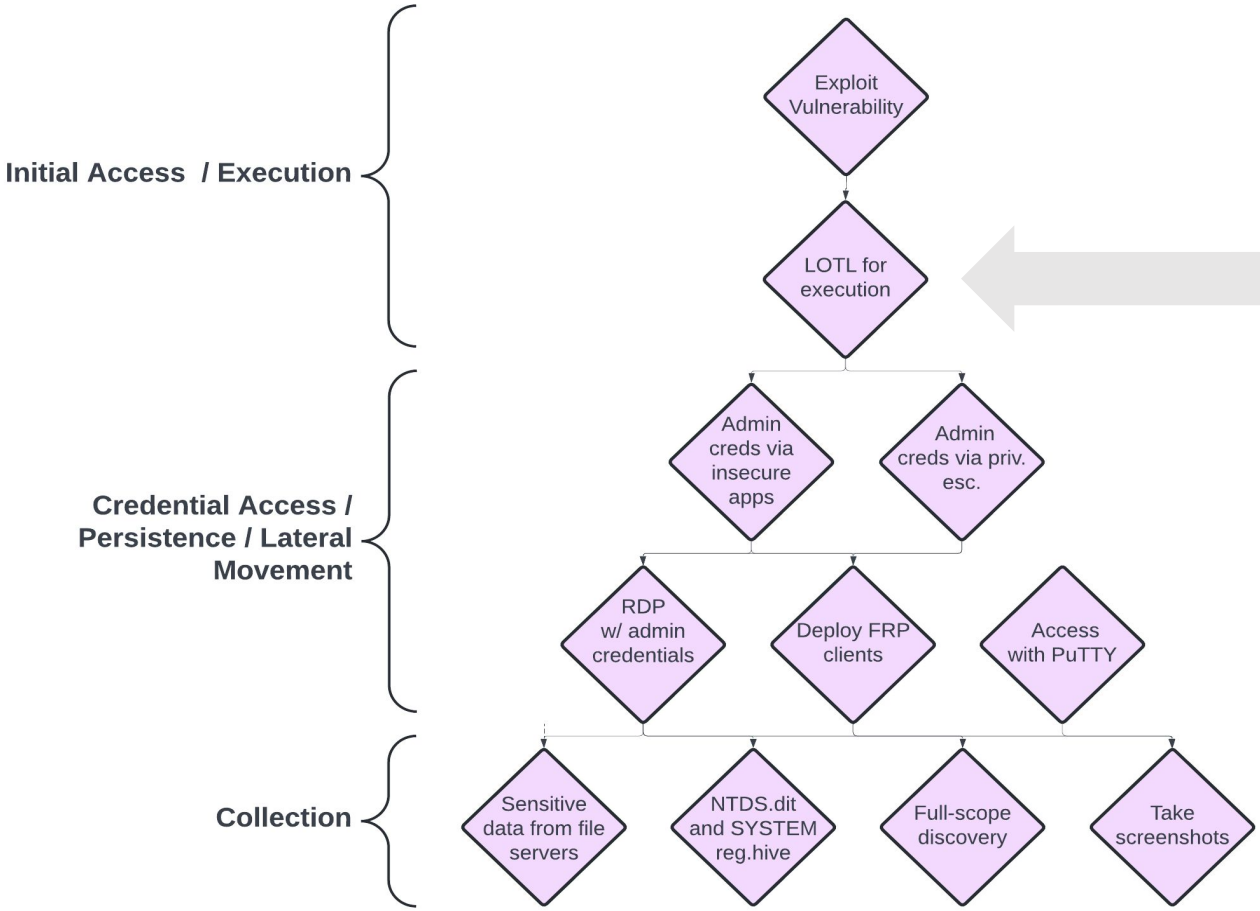


Source:

- https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a
- https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/

Preliminary	⛔	Deliberate	✅	Indepth	✅

TTP Mapping to Attack Tree



Adversary

Volt Typhoon

Capability

T1133: Ext. Remote Services
T1059.001: PowerShell
T1078: Valid Accounts

Infrastructure

Compromised SOHO network devices

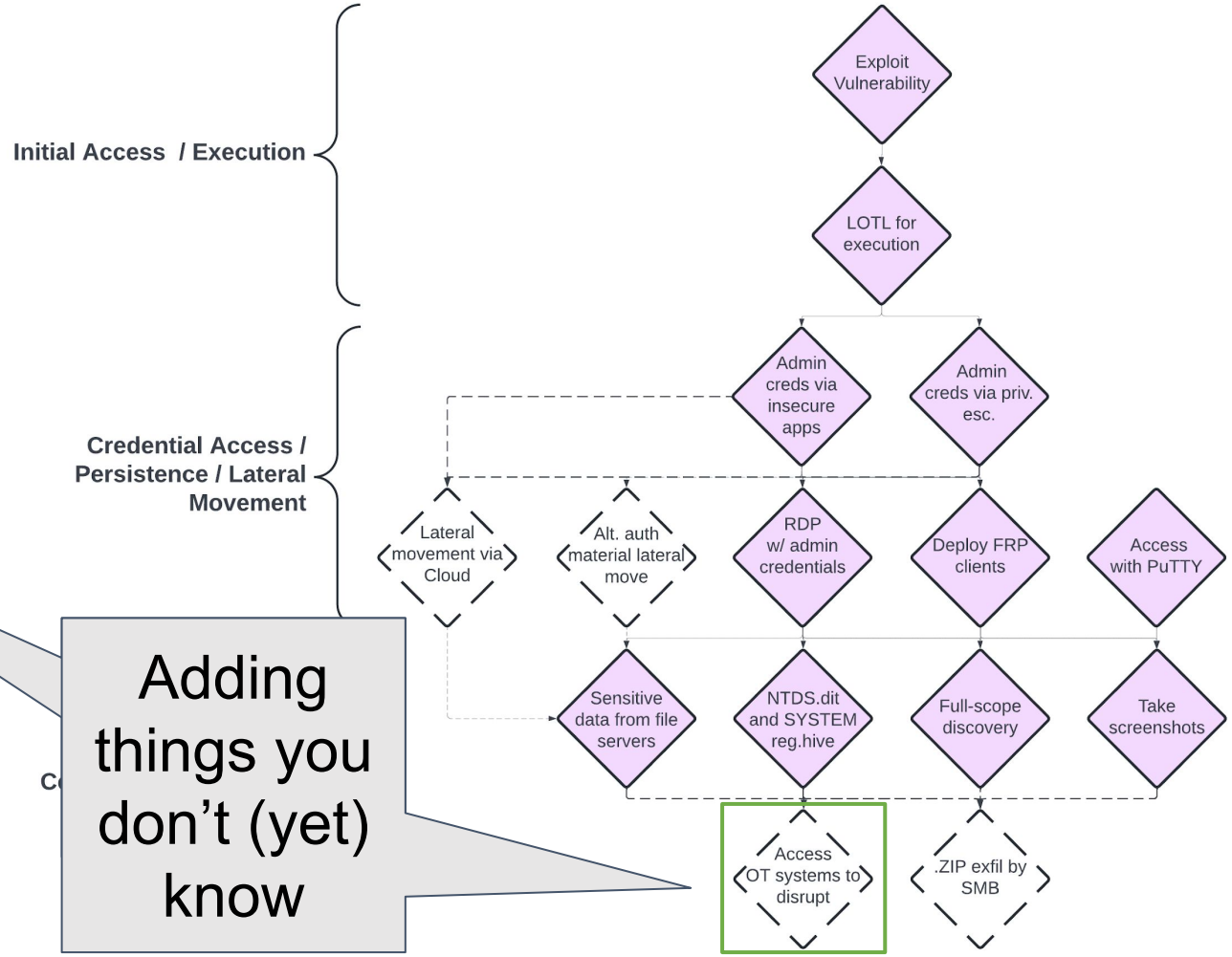
IP:XXX.XXX.XXX.X

Victim

Windows Servers

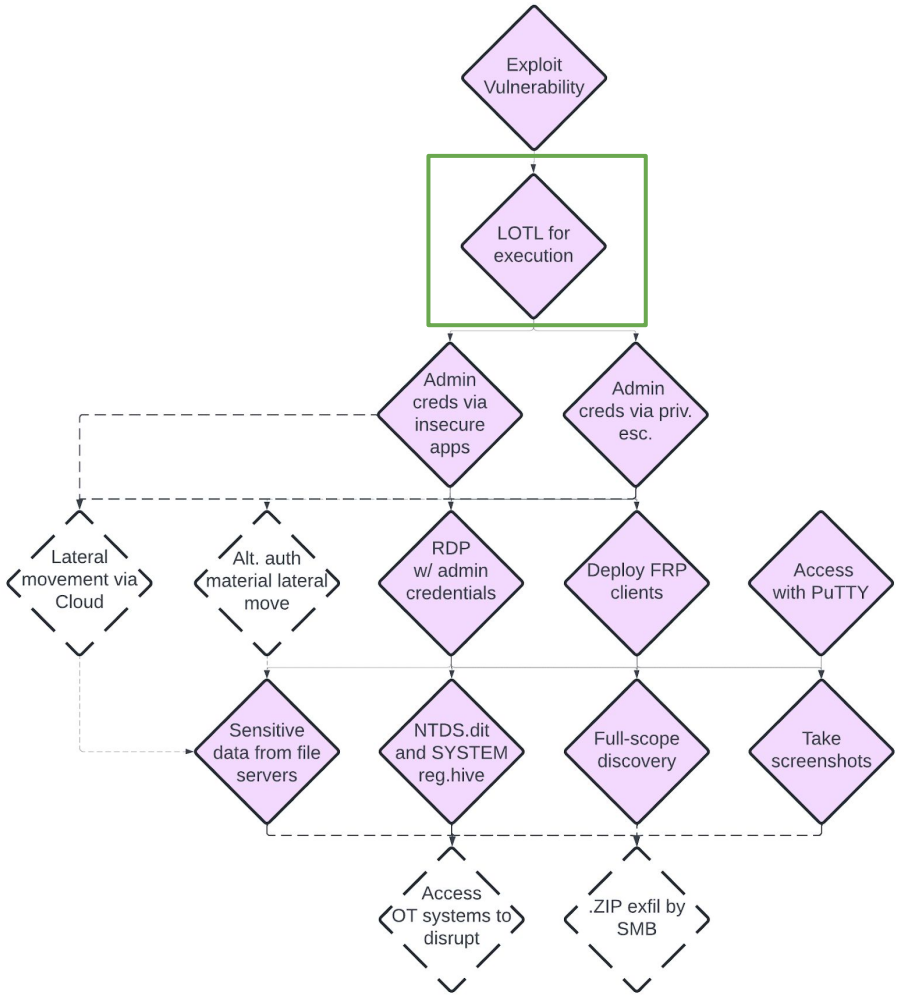
Adding Postulated Events

8. **Volt Typhoon uses elevated credentials for strategic network infiltration and additional discovery, often focusing on gaining capabilities to access OT assets.** Volt Typhoon actors have been observed testing access to domain-joint OT assets using default OT vendor credentials, and in certain instances, they have possessed the capability to access OT systems whose credentials were compromised via `NTDS.dit` theft. This access enables potential disruptions, such as manipulating heating, ventilation, and air conditioning (HVAC) systems in server rooms or disrupting critical energy and water controls, leading to significant infrastructure failures (in some cases, Volt Typhoon actors had the capability to access camera surveillance systems at critical infrastructure facilities). In one confirmed compromise, Volt Typhoon actors moved laterally to a control system and were positioned to move to a second control system.



Preliminary	⛔	Deliberate	✅	Indepth	✅

Prioritization Assessment Example



Adversary

Volt Typhoon

Capability

T1133: Ext. Remote Services
T1059.001: PowerShell
T1078: Valid Accounts

Infrastructure

Compromised SOHO network devices

IP:XXX.XXX.XXX.X

Victim

Windows Servers

Prevalence & Choke Point Example

Super prevalent example

Table 8: Volt Typhoon actors ATT&CK Techniques for Enterprise

Execution		
Technique Title	**ID**	**Use**
Command and Scripting Interpreter	T1059	Volt Typhoon uses hands-on-ke ecution for their malicious activity via the command-line.
Command and Scripting Interpreter: PowerShell	T1059.001	Volt Typhoon has executed clients via PowerShell.
Command and Scripting Interpreter: Unix Shell	T1059.004	Volt Typhoon has used `Brightmetricagent.exe`, which contains multiplexer libraries that can bi-directionally stream data over through NAT networks and contains a command-line interface (CLI) library that can leverage command shells such as PowerShell, Windows Management, Instrumentation (WMI), and Z Shell (zsh).

D	F	G	H	I	J	K	L
	Choke Point						
Technique (Name)	**Num. TID Before**	**Num. TID Afte**	**Choke Point**	**Be**	**Before**	**After Uti**	**After Utilit**
Scheduled Task/Job	7	5	0.6	0.7	0.7	0.5	0.5
Command and Scripting Interpreter	10	15	1	1	1	1.5	1
Impair Defenses	1	1	0.1	0.1	0.1	0.1	0.1
Process Injection	3	6	0.45	0.3	0.3	0.6	0.6
Masquerading	1	1	0.1				
Signed Binary Proxy Execution	1	1					
Hijack Execution Flow	4	3					

Force choke target

Sources: https://top-attack-techniques.mitre-engenuity.org/ & https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

Actionability Assessment Example

Amount of readily available Splunk content

Security Con

Content by Tag

Splunk Enterprise	1581	Splunk Enterprise Security	1372	Splunk	
Defense Evasion	991	Endpoint	733	Privile	
Persistence	516	Initial Access	325	Creden	
Execution	289	Discovery	266	Impair Defenses	97
Lateral Movement	86	Impact	85	Command And Control	83
Splunk Behavioral Analytics	74	Command and Scripting Interpreter	73	System Binary Proxy Execution	73
Disable or Modify Tools	71	Collection	69	Exploit Public-Facing Application	68
Resource Development	67	Valid Accounts	62	Web	61
Modify Registry	61	Cloud Accounts	59	Abuse Elevation Control Mechanism	57
Brute Force	43	PowerShell	42	Exfiltration	41
Account Discovery	41	OS Credential Dumping	39	Phishing	39
User Execution	39	Spearphishing Attachment	36	External Remote Services	34

74 Command and Scripting Interpreter 73

ty 71 Collection 69

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

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

Search

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			
CA-08				
CM-05	Access Restrictions for Change			

Showing 1 to 10 of 24 rows 10 rows per page

NIST 800-53 Controls

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

Preliminary	✅	Deliberate	✅	Indepth	✅

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

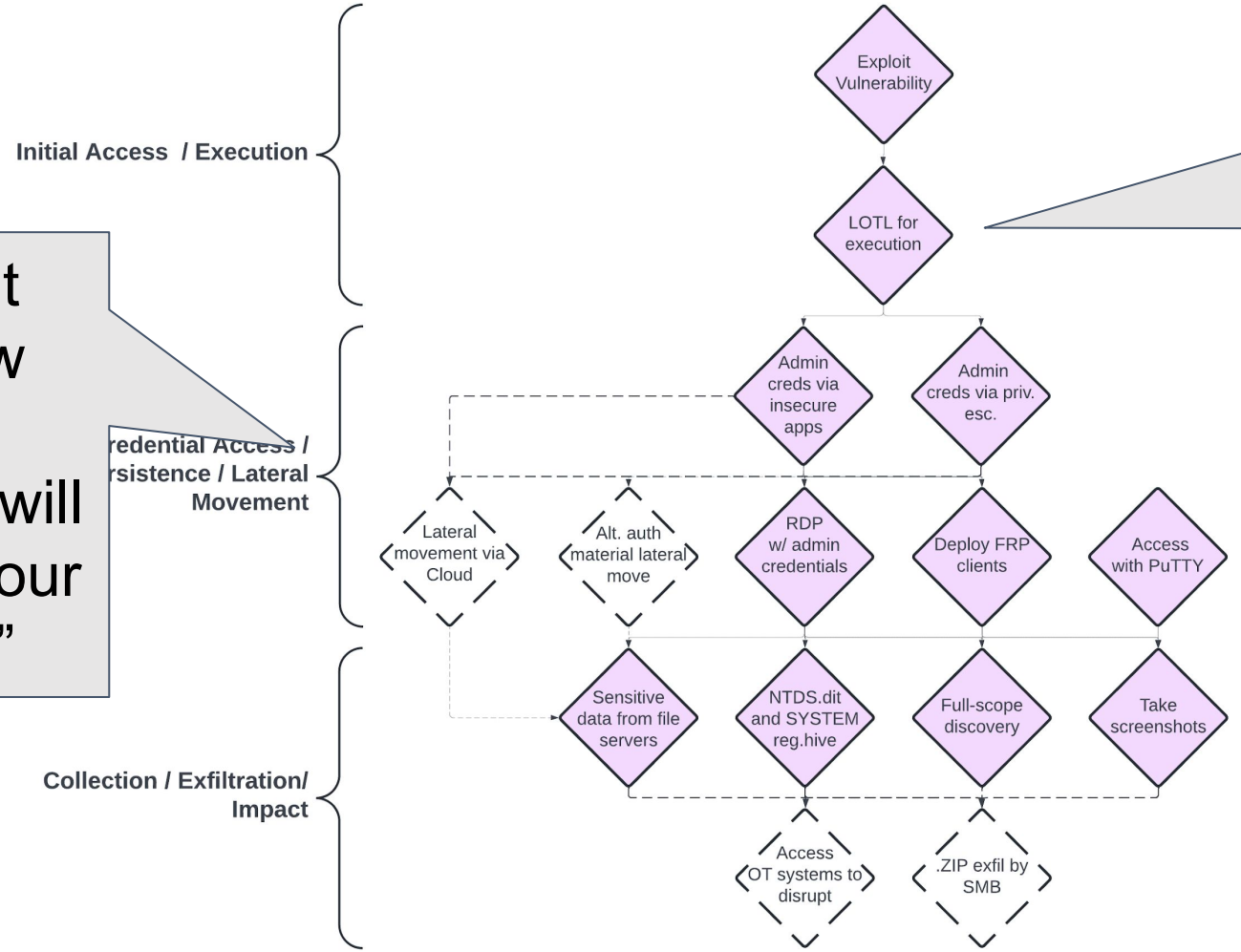
Source: https://research.splunk.com/tags/#external-remote-services & https://center-for-threat-informed-defense.github.io/mappings-explorer

Example questions:

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

Preliminary	✅	Deliberate	✅	Indepth	✅

Conscious Prioritization



"We don't know how lateral movement will play out in our scenario"

"We know exactly how to this element will be prevented"

Wrapping it up

What Attack Trees are Really About

A mental model, evolving based on new innovations

Find us for questions through the following channels

Sherman Chu

Threat-Informed Defense Advocate
Warhammer Nerd

@aperturenoise
/shermanchu1

Gert-Jan Bruggink

Cyber threat cartographer
CTI Bob Ross
Cyber weatherman
Lego afficionado

@gertjanbruggink
github.com/gertjanbruggink
/gertjanbruggink

Thank You!

FIRST™
Improving Security Together