

# Update on Attack Flow

Mark Haase

MITRE Center for Threat-Informed Defense

May 15, 2025 • Brussels



# Together, we are changing the rules of the game



# + MITRE

## Membership is:

- ✓ Highly-sophisticated
- ✓ Global & cross-sector
- ✓ Non-governmental
- ✓ Committed to collaborative R&D in the public interest



## PROBLEM

Defenders often track adversary behaviors atomically, focusing on one specific action at a time. This makes it harder to understand adversary attacks and to build effective defenses against those attacks.



## SOLUTION

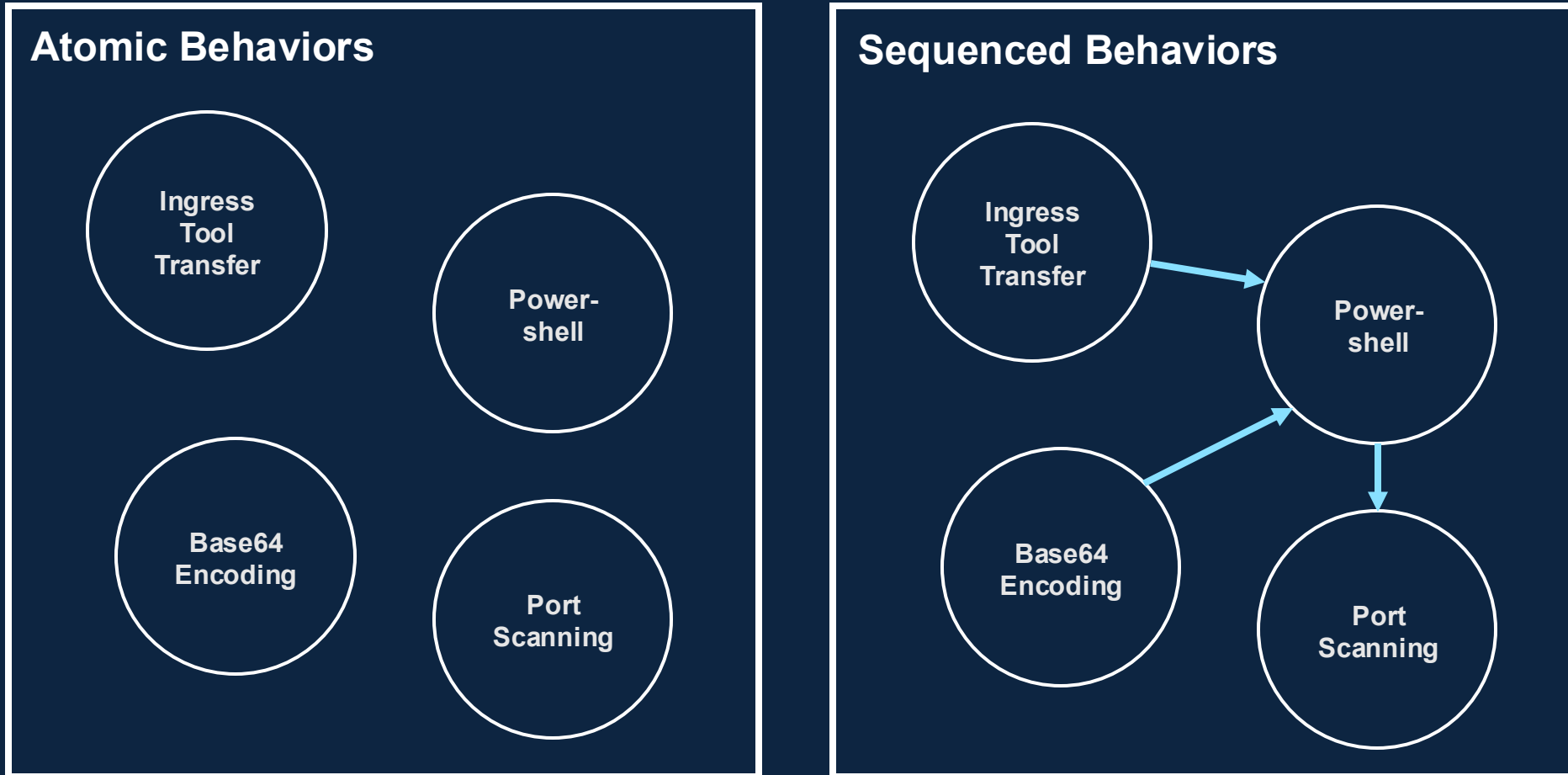
Create a language, and associated tooling, to describe flows of ATT&CK techniques and combine those flows into patterns of behavior.



## IMPACT

Help defenders and leaders understand how adversaries operate and compose atomic techniques into attacks to better understand defensive posture.


# Atomic Behaviors vs Sequences




# Tesla Incident: Atomic Behaviors

## Tesla cloud systems exploited by hackers to mine cryptocurrency

Updated: Researchers have discovered that Tesla's AWS cloud systems were compromised for the purpose of cryptojacking.



Written by **Charlie Osborne**, Contributor  
Posted in Zero Day on February 20, 2018 | Topic: Security




Tesla

Tesla's cloud environment has been exploited by threat actors to mine cryptocurrencies, researchers have discovered.

On Tuesday, cloud security firm **RedLock** released the firm's **2018 Cloud Security Trends** report which documents the discovery of an unprotected Kubernetes console belonging to automaker Tesla.

The Kubernetes console is used to automate the deployment,




**RELATED**

- Best Java bootcamps: Where to learn Java (and why you should!)
- The 9 best cloud storage services: Cost, free storage, and features compared
- The best smart speakers: Should you go with Alexa, Siri, or Google Assistant?

**SECURITY**

Hackers spent months inside a network and nobody noticed. Then a ransomware gang turned up

**Ad**



Secure employees at scale  
Say goodbye to password spreadsheets

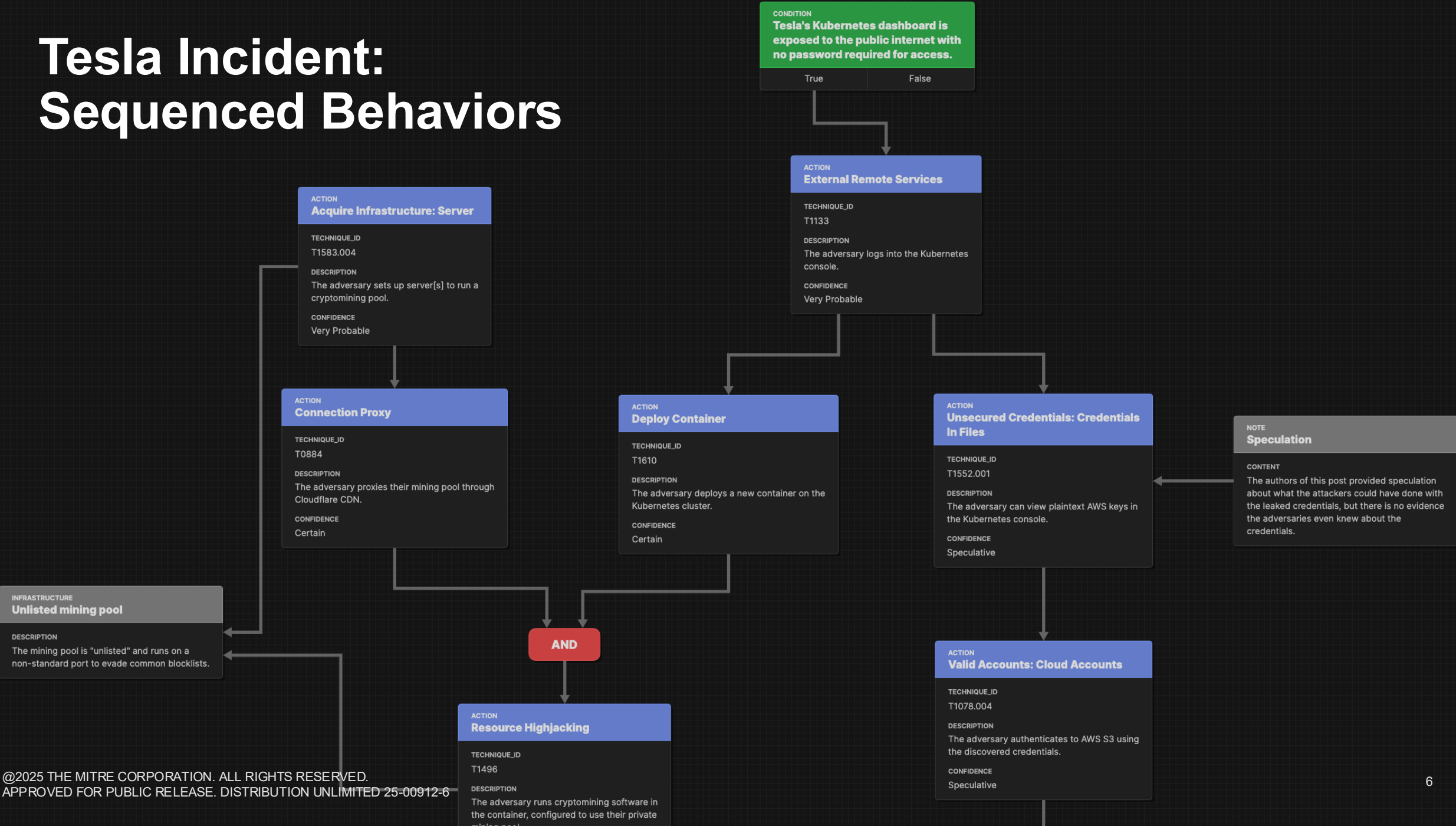
1Password [Learn More](#)



Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 16 techniques
Active Scanning (8/3)	Acquire Infrastructure (0/4)	Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation (0/5)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Adversary-in-the-Middle (0/3)
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/4)	<b>External Remote Services</b>	<b>Deploy Container</b>	Boot or Logon Autostart Execution (0/14)	Boot or Logon Autostart Execution (0/14)	BITS Jobs	Credentials from Password Stores (0/5)
Gather Victim Network Information (0/4)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Build Image on Host	Exploitation for Credential Access
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/8)	Inter-Process Communication (0/3)	Browser Extensions	Create or Modify System Process (0/4)	Decfuscate/Decode Files or Information	Forced Authentication
Phishing for Information (0/2)	Obtain Capabilities (0/4)	Replication Through Removable Media	<b>Native API</b>	Compromise Client Native API (T1108)	Domain Policy Modification (0/2)	<b>Deploy Container</b>	Forge Web Credentials (0/2)
Search Closed Sources (0/2)	Stage Capabilities (0/5)	Supply Chain Compromise (0/3)	Scheduled Task/Job (0/4)	Create Account (0/2)	Escape to Host	Direct Volume Access	Input Capture (0/4)
Search Open Technical Databases (0/4)		Trusted Relationship	Shared Modules	Create or Modify System Process (0/4)	Event Triggered Execution (0/15)	Domain Policy Modification (0/2)	Modify Authentication Process (0/5)
Search Open Websites/Domains (0/2)		Valid Accounts (1/4)	Software Deployment Tools	Event Triggered Execution (0/15)	Exploitation for Privilege Escalation	Execution Guardrails (0/1)	Multi-Factor Authentication Interception
Search Victim-Owned Websites			System Services (0/2)	<b>External Remote Services</b>	Hijack Execution Flow (0/12)	Exploitation for Defense Evasion	Multi-Factor Authentication Request Generation
			User Execution (0/3)	Hijack Execution Flow (0/12)	Process Injection (0/12)	File and Directory Permissions Modification (0/2)	Network Sniffing
			Windows Management Instrumentation	Implant Internal Image	Scheduled Task/Job (0/5)	Hide Artifacts (0/18)	OS Credential Dumping (0/8)
				Modify Authentication Process (0/5)	Valid Accounts (1/4)	Hijack Execution Flow (0/12)	Steal Application Access Token
				Office Application Startup (0/4)		Impair Defenses (0/4)	Steal or Forge Kerberos Tickets (0/4)
				Pre-OS Boot (0/5)		Indicator Removal on Host (0/4)	Steal Web Session Cookie
				Scheduled Task/Job (0/5)		Indirect Command Execution	Unsecured Credentials (0/7)
				Server Software Component (0/5)		Masquerading (0/7)	
				Traffic Signaling (0/1)		Modify Authentication Process (0/5)	
				Valid Accounts (1/4)		Modify Cloud Compute Infrastructure (0/4)	



# Tesla Incident: Sequenced Behaviors

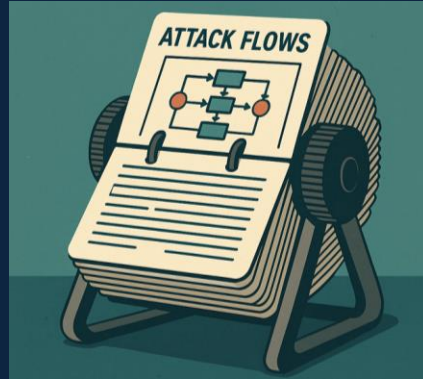


# What's Included?



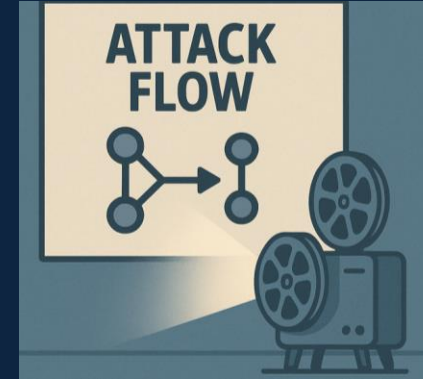
## Attack Flow Builder

Web-based tool for creating, editing, and presenting flows.



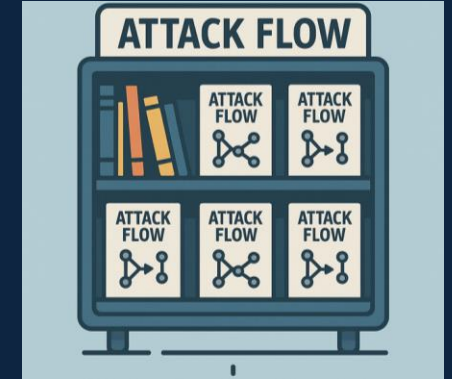
## Flow Library

A collection of 34 example flows, useful for learning about Attack Flow, learning about breaches, and data mining.



## Visualization

Tools for visualizing flows for different audiences and purposes.



## Documentation

User-friendly introduction to flow, easy access to the library and tools.

← Machine Readable (STIX) Data →

# Who is using Attack Flow?

- Global community from US to EU to APAC.
- Multinational corporations and small business.
- Threat modelers, red teamers, CTI analysts, defenders.

**Dave Johnson** · 1st  
Threat Intelligence Advisor @Feedly | Former FBI Analyst | Entrepren...  
1mo · Edited · 🌐

I've been working on a secret ATT&CK Flow visualization tool 🤖

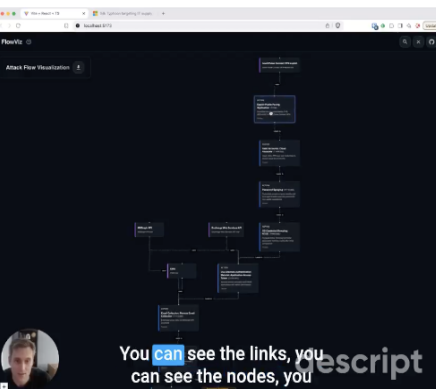
Why? Because it's winter in Wisconsin. 🌨️

What does it do? It generates a graph of attack procedures in a threat intelligence report automatically, so you get the gist of detailed reports much faster.

It will also generate STIX bundles so you can do adversary emulation in tools like MITRE Caldera. Or, you can export into an image file to use in a custom report or presentation.

Drop a comment down below if your interested! 🙌

#ThreatIntelligence #AdversaryEmulation #ATTACKFlow  
#CyberSecurity



You can see the links, you can see the nodes, you can see the flow

You and 421 others · 112 comments · 19 reposts

Like · Comment · Repost · Send

**Dewank Pant** · 1st  
Security@Amazon (Alexa AI Security Research) | Lea...  
(edited) 1mo · ...

**Dave Johnson** This is great! would love to collaborate on this. Some thoughts: these attack flow details could also be linked to an exploit crafting agent to generate new attack variants, speeding up security testing. This would also be valuable for prompt testing tools (like Garak, and Pyrit), as jailbreak research papers come out every other day, this way we could feed in new papers and generate multiple attack variants to expand the test sets!

**David Greenwood** · 1st  
I build products that make threat intelligence analysts go; "Wow! That's wh...  
2mo · 🌐

txt2stix now supports automated Attack Flow extraction for MITRE ATT&CK references in reports.

I've update the last part of my blog post (linked in the post below) with some examples.

**dogesec**  
1,765 followers  
2mo · Edited · 🌐

For a long time, I, like many of you, have been tagging detection content with ATT&CK Techniques.


Sometimes, ashamedly, I tout full detection coverage for a particular threat. I show off the ATT&CK Navigator highlighting how all the detections cover the ATT&CK Techniques an intel team has discovered an adversary to use

The reality is, although this captures a lot of information, and is often better-than-nothing, it still lacks a key component – time (or flow!) of techniques.

Many people incorrectly read the ATT&CK Matrix as a flow. They assume the flow of an attack moves from left to right. This is incorrect in many instances where an attacker jumps backwards and forwards in their attempts to achieve an objective.

The point is this; the ATT&CK Matrix alone does not provide enough to describe how an adversary might work and that's where Attack Flows come in.

<https://lnkd.in/ezaPN4rB>



**Beyond the ATT&CK Matrix: How to Build Dynamic Attack Flows with STIX**  
dogesec.com

**Gert-Jan Bruggink** · 1st  
Founder & CEO, Venation | Proven Systems for Smarter Decisions.  
Visit my website  
2mo · Edited · 🌐

I've been successfully modeling threat scenarios for over 7 years. Here's how I recently updated my 'system' with Attack Flow:

I believe that cybersecurity needs a support function that helps understand variables (threats) that drive risk + support explicit decision making on what to do about it.

To do this right, you need a system.

Most teams understand WHY you need to do this. Some even have figured out HOW. Today, I'll show you WHAT you can do right now to integrate this in your daily workflow using Attack Flow.

Copy it into your internal procedures and create your own!

Let's make this week count!

Gert-Jan

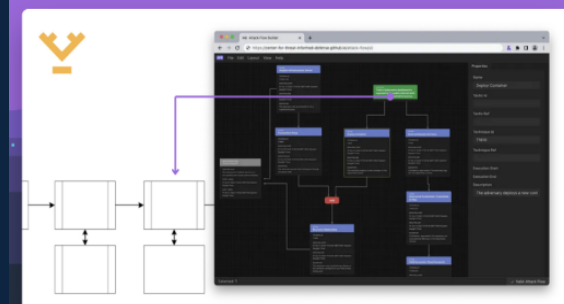
If you want systems directly in your mailbox, join our newsletter for the complete ones:

GO here: <https://lnkd.in/eWwxc5bQ>

Found my content useful?

Share it with your network & follow [Gert-Jan Bruggink](#) and [Venation](#) for more. 🍷

#CyberSecurity #RiskManagement #ThreatModeling #ThreatScenarios





# What's next?

## Attack Flow 3.0

July 8<sup>th</sup> 2025

- Refined look and feel
- Dark and light modes
- Blog mode: embed interactive flows on web pages
- Import STIX bundles
- Numerous efficiency and productivity improvements
- Fully backwards compatible

TECHNIQUE ID  
T1059.001

DESCRIPTION  
Within the malicious files, encoded PowerShell scripts are used to download additional malicious scripts.

CONFIDENCE  
Certain

ACTION  
**Hijack Execution Flow: DLL Search Order Hijacking**

TECHNIQUE ID  
T1574.001

TECHNIQUE REF  
attack-pattern--2fee9321-3e71-4cf4-af24-d4d40d355b34

DESCRIPTION  
Black Basta uses Qakbot DLL files, which can exploit the Windows 7 calculator to execute malicious payloads.

CONFIDENCE  
Certain

MALWARE  
**Qakbot**

DESCRIPTION  
aka Qbot; Windows malware strain that has evolved into a malware dropper

MALWARE TYPES  
dropper

IS FAMILY  
True

CAPABILITIES  
communicates-with-c2,  
installs-other-components

ACTION  
**System Binary Proxy Execution: Regsvr32**

TACTIC ID  
TA0005

TECHNIQUE ID  
T1218.010

DESCRIPTION  
regsvr32.exe is used to execute a malicious

# Thank You



<https://ctid.mitre.org>