Threat Models, Landscape, and Profiles Oh My

Wade Wells - WadingThruLogs

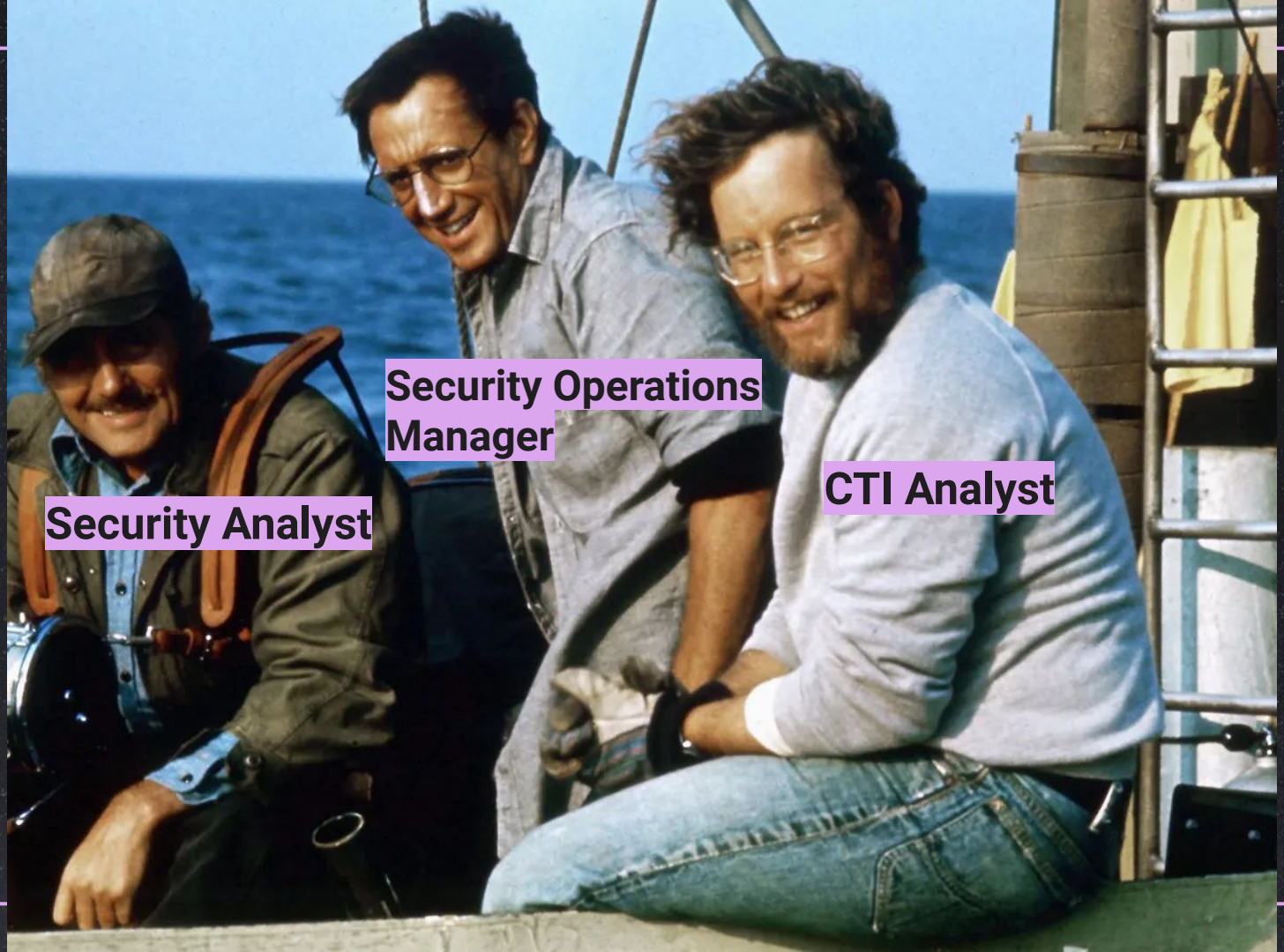
8 Years of SecOps (Threat Hunting, Threat Intel, Detection Engineering) in Financials and MSSP

MS - Cybersecurity Georgia Tech, Several certs

BSides San Diego Board, Talkin' Bout News, BHIS Community Leader, Antisyphon Trainer

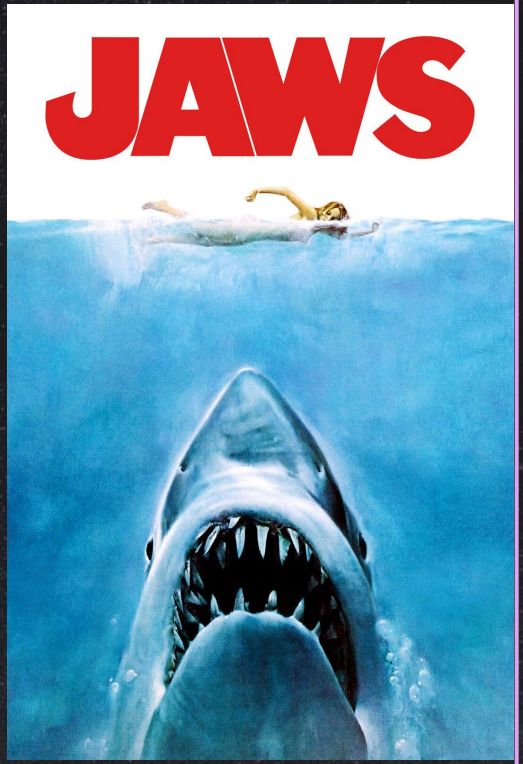
START WITH AN ANALOGY

- All thoughts are coming from a defense perspective, but can be applied in multiple ways.


Security Operations Manager
Security Analyst
CTI Analyst

EXAMPLE: JAWS

- The mayor understands that Amity Island's weakness is the loss of tourism (**Modeling**)
- Hooper understands sharks as well as the importance of watching the coastline (**Landscape**)
- Brody, Hooper, and Quint were sent to neutralize the threat but underestimated the issue (**Profiling**)



Modeling, Landscaping, and Profiling

Looking at **you**

Looking **out there**

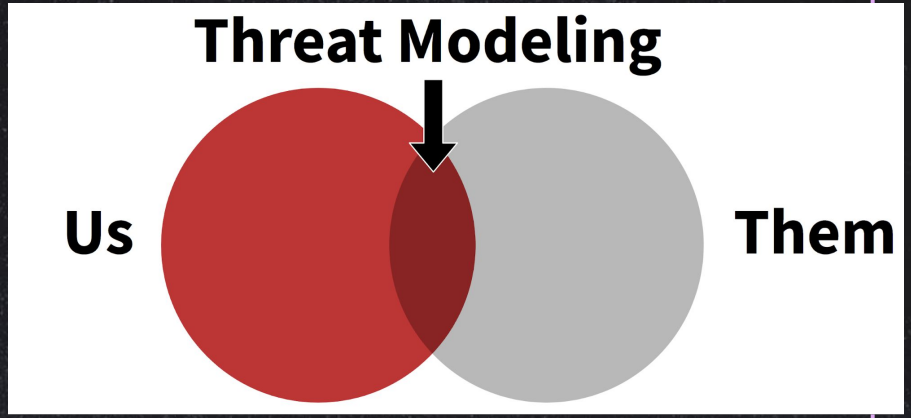
Looking at **them**

THREAT MODELING

THREAT MODELING

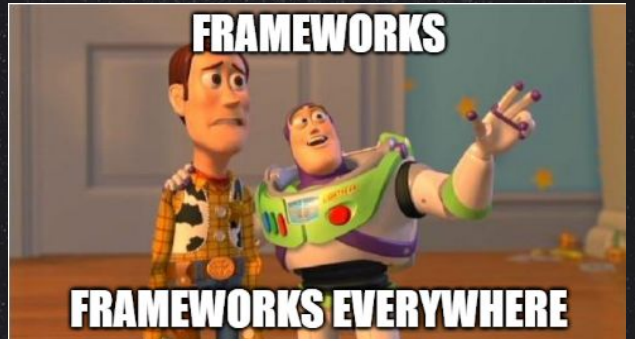
A risk assessment that models organizational strengths and weaknesses

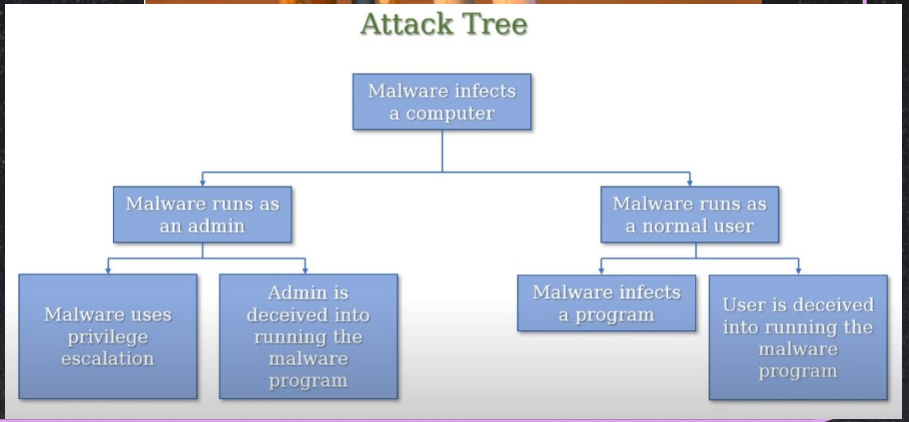
- What do you want to protect?
- Who do you want to protect it from?
- How likely does it need protection?
- How dire are the consequences if you fail?
- How much effort are you willing to go through to try to prevent those?



THREAT MODELING FRAMEWORKS

- STRIDE (Spoofing, Tampering Repudiation, Information disclosure, Denial of service, Elevation of privilege)
- PASTA (Process for Attack Simulation and Threat Analysis)
- Attack Trees

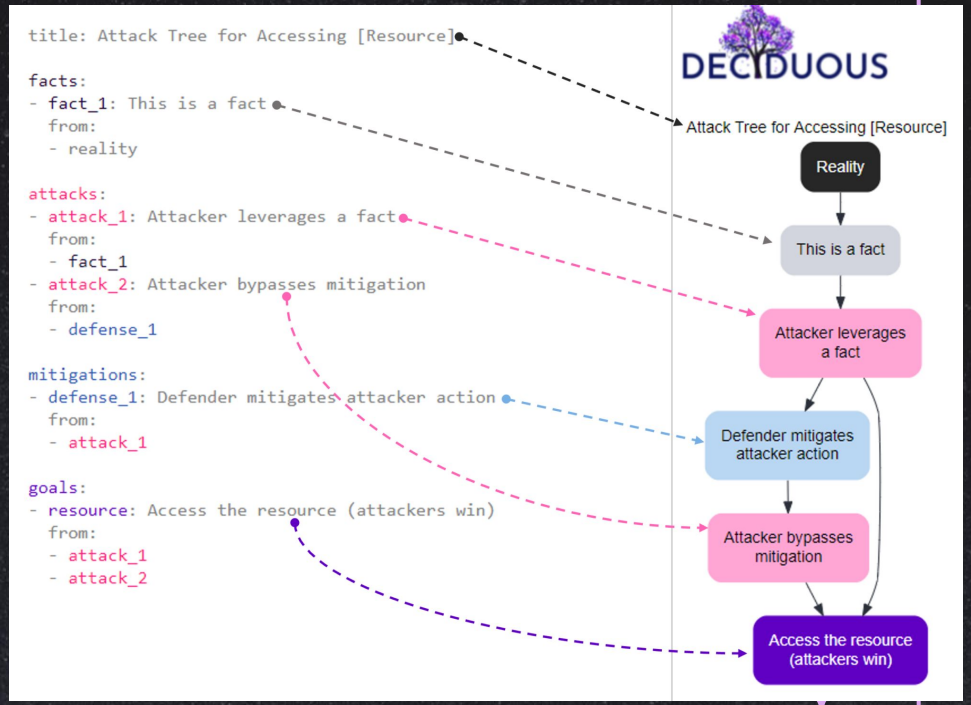




STRIDE GPT

DECIDUOUS

- Analyzing and visualizing adverse scenarios/attack decisions
- Interactive and User-Friendly
- Customization and Styling
- Open Source

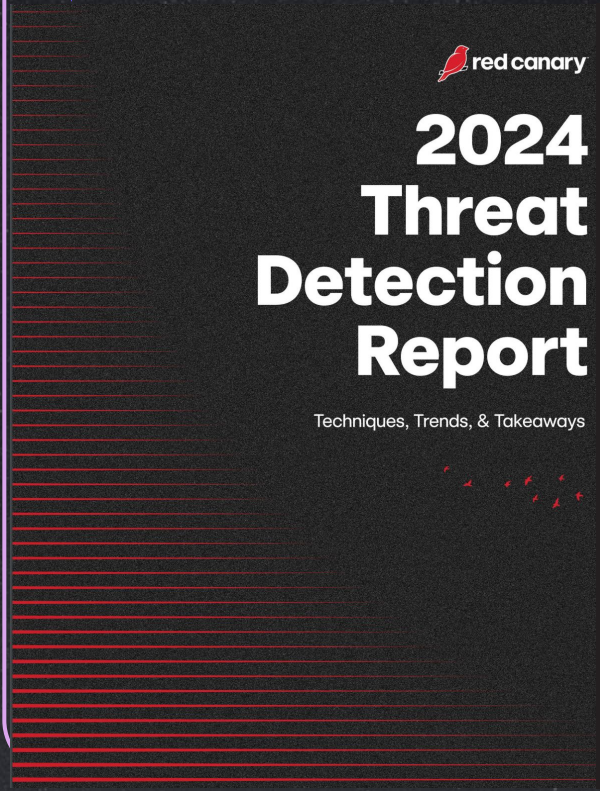


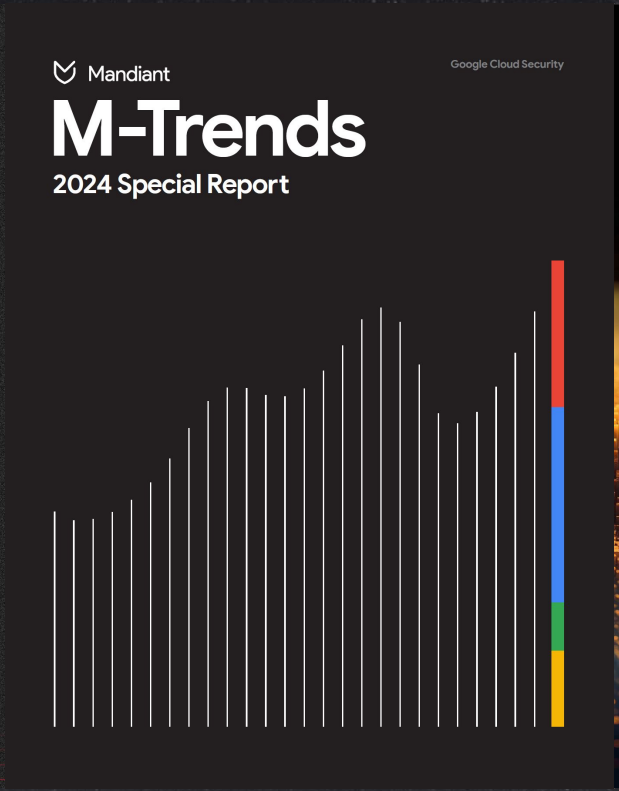
THREAT LANDSCAPING

THREAT LANDSCAPING

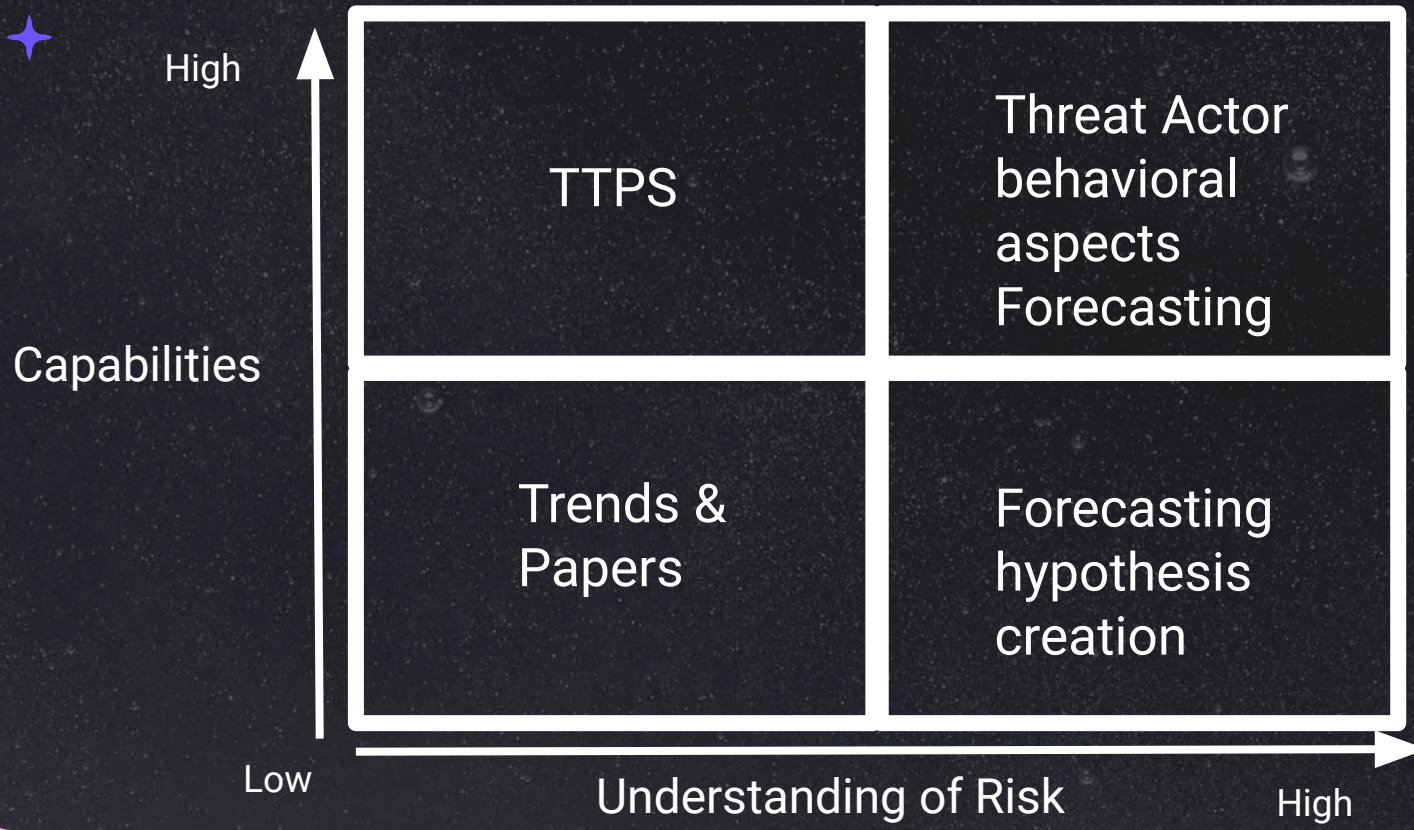
- What is going on out there?
  - What's hot right now?
  - Is there a possible invasion of a country your company works in?
- Does it relate to my Org?
- Learn from others mistakes:
  - Password in chat?
  - Okta misconfigured?

Annual Security Reports





EXPECTATIONS



The Joy of Threat Landscaping - Gert-jan Bruggink

THREAT LANDSCAPE TOOLS

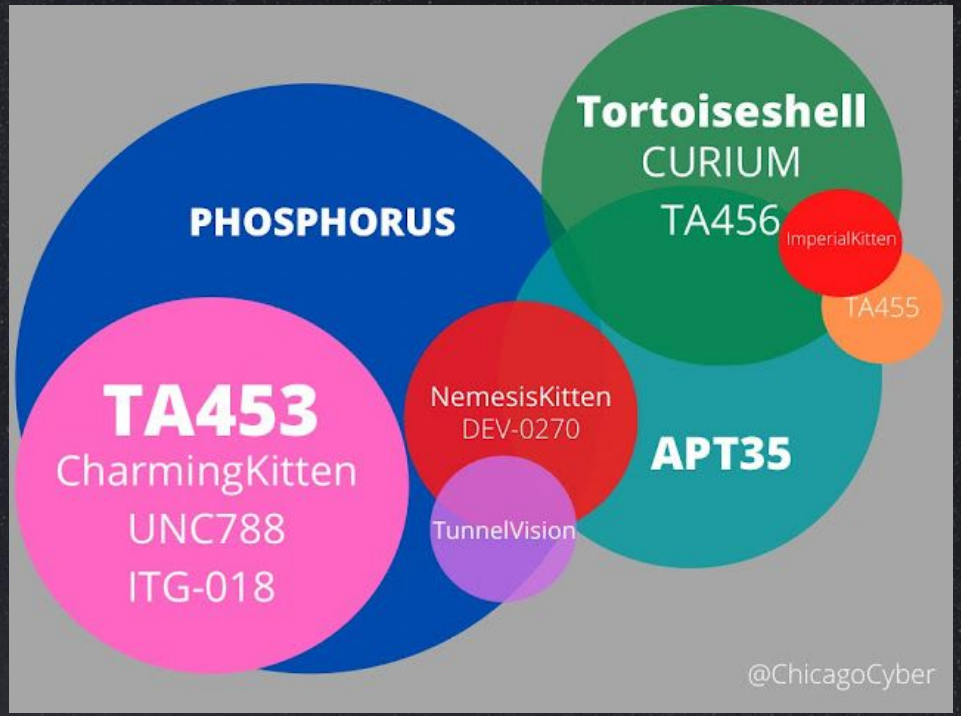
- Social Media
  - Twitter list
- Start.me
- Dragon News Bytes
- Google News Alerts
- CISA KEV

THREAT ACTOR & PROFILING

What is a Threat Actor Anyway?

- Financially motivated
- Nation-state
- Ideologues (Hacktivists and Terrorists)
- Thrill seekers and trolls
- Insiders and Competitors

Naming & Attribution



BY THE NUMBERS

Too Many Threats

Mandiant *indicates* it currently tracks 3,500 threat groups in 2023, an increase of 900 from the previous year. The firm also started tracking 588 new malware families in 2022.

In 2023, Microsoft *indicated* that it tracks ***300 unique threat actors***, including ***160 nation state actors*** and ***50 ransomware groups***

In 2021, Google's Threat Analysis Group *announced* that it tracks ***more than 270 government-sponsored actor groups*** associated with ***more than 50 countries***

Tidal's analysis of public extortion threats identified ***56 ransom groups*** that maintained extortion sites in 2022 & 2023

Tidal Cyber -Cyber Threat Profiling

Threat Actor Profiling Benefits

- Executives Understanding
- Review Security Architecture
- Focusing on Threats Proactively
- Enhance Threat Modeling
- Threat Activity in Our Environment

PROFILING FOR A FINTECH

Who is Attacking:

- Your Sector
- Your Rivals
- Customers/Data
- Your Region

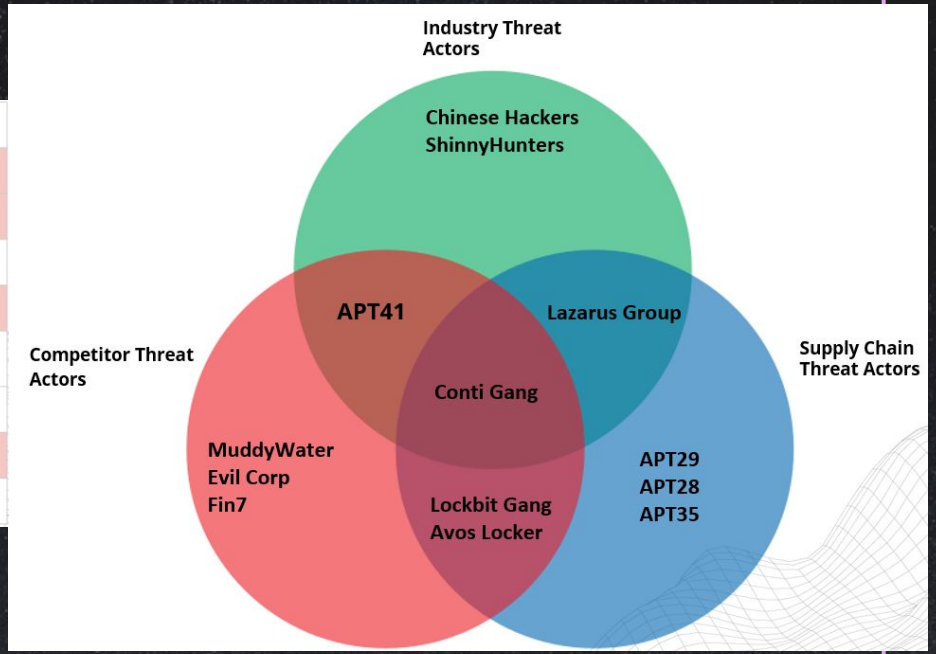
Competitor Threat Actors	*Industry Threat Actors*	*Supply Chain Threat Actors*
LockBit Gang	Chinese Hackers	Conti Gang
AvosLocker Ransomware Group	Lazarus Group	Lazarus Group
MuddyWater	ShinyHunters	APT29 The Dukes
APT41	Conti Gang	LockBit Gang
Conti Gang	Hotarus Corp	APT28
Cyber Partisans	North Korean Hackers	APT35
Evil Corp	AgainstTheWest	AvosLocker Ransomware Group
FIN7	APT41	FamousSparrow

INTENT & WILLINGNESS

A	B	C
	Why would this actor target this organization with this type of attack?	
5	Target-Specific Data:	$ACTOR targets $ORG based on an objective that can only be achieved within $ORG's network
4	Ideology Association:	$ACTOR targets $ORG based on its association with a specific ideology (e.g., USG, war, etc.)
3	Sector Association:	$ACTOR targets $ORG based on its association with a specific business sector (e.g., finance, energy, government)
2	Regional Association:	$ACTOR targets $ORG based on its regional area of operations (e.g., North America, Middle East, etc.)
1	Target of Opportunity:	$ACTOR targets $ORG simply as a target of opportunity
	Willingness modifier: What constraints may impact the actor's intent?	
0	Strained diplomatic relations/previous hostilities/significant economic disruption perceived by $ACTOR from $ORG's operations	
-1	Moderate relations with the U.S. and moderate economic dependencies between $ACTOR interests and $ORG's operations	
-2	Strong diplomatic, economic, and security ties with the US	

24 TO 13

Competitor Threat Actors	*Industry Threat Actors*	*Supply Chain Threat Actors*
LockBit Gang	Chinese Hackers	Conti Gang
AvosLocker Ransomware Group	Lazarus Group	Lazarus Group
MuddyWater	ShinyHunters	APT29 The Dukes
APT41	Conti Gang	LockBit Gang
Conti Gang	Hotarus Corp	APT28
Cyber Partisans	North Korean Hackers	APT35
Evil Corp	AgainstTheWest	AvosLocker Ransomware Group
FIN7	APT41	FamousSparrow



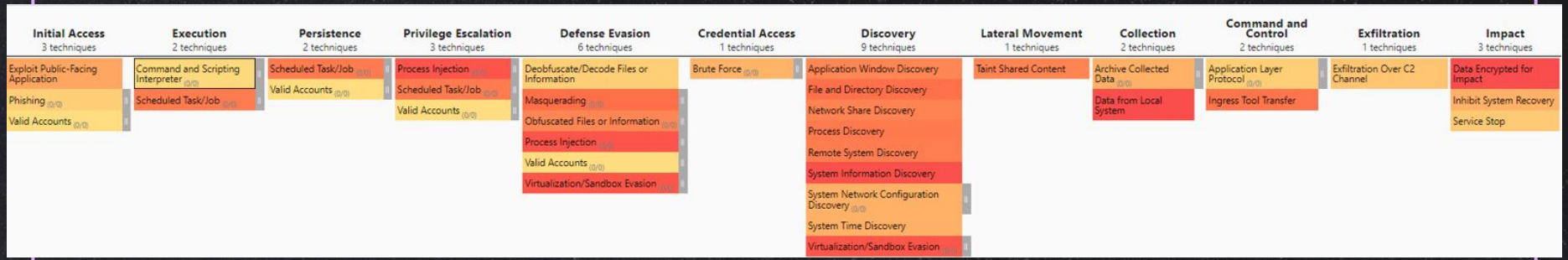
CAPABILITIES & NOVELTY

	Capability: What evidence is available that this actor is capable of this attack type?	
5	Significant Capability	Significant evidence that $ACTOR previously conducted this type of activity; multiple trusted sources confirmed
4	Credible Capability	Credible evidence of operational capability; moderately confirmed
3	Limited Capability	Some evidence of operational capability; limited sources
2	Possible Capability	Very limited evidence of operational capability; feasibility confirmed
1	Not Capable	No evidence of operational capability; feasibility unconfirmed
	Novelty modifier: What indication of advanced skills are evident?	
0	Custom toolset per campaign with demonstrated living off the land capability	
-1	Limited availability/high-cost toolset used in multiple campaigns	
-2	Toolset generally available	

INTENT AND CAPABILITIES

Actor	Alias	Intent	Capability	Category	Lists
LockBit Gang	BITWISE SPIDER	3	3.5	Financially Motivated, Ransomeware group	Comp, ,SC
AvosLocker Ransomware Group		3	3.5	Financially Motivated, Ransomeware group	Comp, ,SC
MuddyWater	(Cobalt Ulster, M	1	4	Nation State, Iran	Comp,
APT41	(Axiom Group, B	1	4	Nation State, China	Comp, , Industry
Conti Gang		3	3.5	Financially Motivated, Ransomeware group, Easter European	Comp, , Industry, SC
Evil Corp	(Dridex Gang, G	3	3.5	Financially Motivated, Russian	Comp,
FIN7	(Carbanak)	3	4	Financially Motivated, State sponsored	Comp,
Chinese Hackers		2	3	Nation State, IP Motivated, industrial information	Industry
Lazarus Group	(HIDDEN COBRA	1	4.5	Nation State, North Korea, Financially Motivated,	Industry, SC
ShinyHunters		2	3	Financially Motivated, Underground Forum, IP and PII theft	Industry
APT29 The Dukes	(Cozer, Cozy Bea	1	4.5	Nation State, Russia, PII	SC
APT28	(Fancy Bear, Iron	1	4.5	Nation State, Russia, espionage	SC
APT35	(Group 83, News	1	4.5	Nation State, Iran,	SC

FINAL FORM


Initial Access
3 techniques
Exploit Public-Facing Application
Phishing (0/0)
Valid Accounts (0/0)
Execution
2 techniques
Command and Scripting Interpreter (0/0)
Scheduled Task/Job (0/0)
Persistence
2 techniques
Scheduled Task/Job (0/0)
Valid Accounts (0/0)
Privilege Escalation
3 techniques
Process Injection (0/0)
Scheduled Task/Job (0/0)
Valid Accounts (0/0)
Defense Evasion
6 techniques
Deobfuscate/Decode Files or Information
Masquerading (0/0)
Obfuscated Files or Information (0/0)
Process Injection (0/0)
Valid Accounts (0/0)
Virtualization/Sandbox Evasion (0/0)
Credential Access
1 techniques
Brute Force (0/0)
Discovery
9 techniques
Application Window Discovery
File and Directory Discovery
Network Share Discovery
Process Discovery
Remote System Discovery
System Information Discovery
System Network Configuration Discovery (0/0)
System Time Discovery
Virtualization/Sandbox Evasion (0/0)
Lateral Movement
1 techniques
Taint Shared Content
Collection
2 techniques
Archive Collected Data (0/0)
Data from Local System
Command and Control
2 techniques
Application Layer Protocol (0/0)
Ingress Tool Transfer
Exfiltration
1 techniques
Exfiltration Over C2 Channel
Impact
3 techniques
Data Encrypted for Impact
Inhibit System Recovery
Service Stop

Threat Actor Resources

- Malpedia Actors
- ATT&CK Groups
- APT Groups and Operations
- Tidal Cyber

CYBER THREAT INTEL 101 CLASS

Incident Response Summit -
Thursday, June 20th, 2024

Wild West Hacking Fest -
Wednesday, October 9th, 2024

A practical approach to threat modeling - Katie Knickles	https://redcanary.com/blog/threat-modeling/
Threat Modeling: 12 Available Methods	https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/
Threat Modeling Cheat Sheet	https://cheatsheetseries.owasp.org/cheatsheets/Threat_Modeling_Cheat_Sheet.html
Deciduous: A Security Decision Tree Generator	https://kellyshortridge.com/blog/posts/deciduous-attack-tree-app/#fnref:1
Stride GPT	https://stridegpt.streamlit.app/
The Joy of Threat Landscaping - Gert-Jan Bruggink	https://youtu.be/Qm5uLzphP3g?si=z5726rc-sRU7jxWW
Intelligence Blogs - Infosecn1nja	https://start.me/p/wMrA5z/cyber-threat-intelligence
Email list - Team Cymru	https://www.team-cymru.com/dnb
Google Alerts	https://www.google.com/alerts
How to set Google Alerts to keep tabs on topics that interest you	https://www.zdnet.com/home-and-office/work-life/how-to-set-google-alerts-to-keep-tabs-on-topics-that-interest-you/
Known Exploited Vulnerabilities Catalog(KEV) - CISA	https://www.cisa.gov/known-exploited-vulnerabilities-catalog
Election Security Spotlight – Cyber Threat Actors - CIS	https://www.cisecurity.org/insights/spotlight/cybersecurity-spotlight-cyber-threat-actors
Threat Group Naming Schemes In Cyber Threat Intelligence - @BushidoToken	https://www.curatedintel.org/2022/05/threat-group-naming-schemes-in-cyber.html
Tidal Cyber -Cyber Threat Profiling	https://github.com/tidalcyber/cyber-threat-profiling
The Threat Actor Profile Guide for CTI Analysts	https://github.com/curated-intel/Threat-Actor-Profile-Guide/blob/main/The%20Threat%20Actor%20Profile%20Guide%20for%20CTI%20Analysts%20v1.1.pdf
Quantifying Threat Actor Assessments I Andy Piazza and Katie Nickels	https://www.youtube.com/watch?v=tcroXAcjdzU&t=1286s&ab_channel=SANSTechnologyInstitute
Quantifying Threat Actors with Threat Box - Andy Piazza	https://klrgrz.medium.com/quantifying-threat-actors-with-threat-box-e6b641109b11
Threat Actors	https://malpedia.caad.fkie.fraunhofer.de/actors
Threat Actors	https://attack.mitre.org/groups/
Threat Actors	https://docs.google.com/spreadsheets/d/1H9_xaxQHpWaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/edit#gid=1864660085
Threat Actors	https://app.tidalcyber.com/groups