



CROWDSTRIKE

**HELP YOUR NON-SECURITY
STAKEHOLDERS**
UNDERSTAND ATT&CK

ELLY SEARLE, LEAD CONTENT STRATEGIST



1

Why we now use ATT&CK to describe detections

2

How we evolved the ATT&CK mental model

3

What it looks like

4

Does it work?





WHY WE NOW USE ATT&CK TO DESCRIBE DETECTIONS

- We got a lot of customer calls asking to explain what detections meant
- Customers found our detection classifications too vague and confusing
- If Falcon admins didn't grasp what detections meant, they definitely couldn't explain to anyone else in their org what adversaries were doing



WHAT OUR CUSTOMERS USED TO GET



Application Compromised



Attacker Methodology



Credential Theft



Data Loss



Data Deletion



Drive-by Download



Establish Persistence



Exploit Pivot



Blocked Exploit



Known Malware



Malicious Document



NGAV



Privilege Escalation



Process Terminated



Ransomware



Server Compromise



Social Engineering



Suspicious Activity



User Compromise



Web Exploit



Evade Detection





WHAT OUR CUSTOMERS USED TO GET

...so we switched to ATT&CK



ATT&CK WAS BETTER, BUT STILL NEEDED **SOME EXPLANATION**

-
- Without context, it's not clear exactly what each tactic means
 - Want anyone to understand what's happening, regardless of security experience
 - People don't need it "dumbed down" – they need context
-





HOW WE EVOLVED THE ATT&CK MENTAL MODEL

- Played with ways to explain concepts to someone capable of learning, but not familiar yet – master/apprentice
- Focused on clear, conversational words





An adversary is trying to _____

ATT&CK tactic	Explain it to a non-security person
Initial Access	Get into your environment
Execution	Run malicious code
Persistence	Maintain their foothold
Privilege Escalation	Gain higher level permissions
Defense Evasion	Avoid detection
Credential Access	Steal logins and passwords
Discovery	Figure out your environment
Lateral Movement	Move through your environment
Collection	Gather data
Exfiltration	Steal data
Command and Control	Control systems





An adversary is trying to _____

ATT&CK tactic	Explain it to a non-security person	Objective
Initial Access	Get into your environment	Gain access
Execution	Run malicious code	Follow through (steal/break)
Persistence	Maintain foothold	Keep access
Privilege Escalation	Gain higher level permissions	Gain (more) access
Defense Evasion	Avoid detection	Keep access
Credential Access	Steal logins and passwords	Gain access
Discovery	Figure out your environment	Explore
Lateral Movement	Move through your environment	Explore
Collection	Gather data	Follow through
Exfiltration	Steal data	Follow through
Command and Control	Contact controlled systems	Contact controlled systems





An adversary is trying to _____

ATT&CK tactic	Explain it to a non-security person	Objective
Initial Access	Get into your environment	Gain access
Credential Access	Steal logins and passwords	Gain access
Privilege Escalation	Gain higher level permissions	Gain (more) access
Persistence	Maintain foothold	Keep access
Defense Evasion	Avoid detection	Keep access
Discovery	Figure out your environment	Explore
Lateral Movement	Move through your environment	Explore
Execution	Run malicious code	Follow through
Collection	Gather data	Follow through
Exfiltration	Steal data	Follow through
Command and Control	Contact controlled systems	Contact controlled systems



THE ADVERSARY IS
TRYING TO OBJECTIVE
BY TACTIC
USING TECHNIQUE.

The adversary is trying to gain access by stealing logins and passwords using credential dumping.

The adversary is trying to keep access by avoiding detection using process hollowing.











HOW WE VALIDATED THE EVOLVED MODEL

-
- Reviewed with internal experts, making sure it didn't get in their way
 - Considered new labels for tactics, but loses value of standardizing
 - Used UX design and research methods to integrate objectives and get feedback from customers
-








FULL CONTEXT IN UI

powershell.exe		 0	 0	 2	 0	 0	 0
SEVERITY	 High  Prevented						
OBJECTIVE	Gain Access						
TACTIC & TECHNIQUE	Credential Access via Credential Dumping						
SPECIFIC TO THIS DETECTION	A PowerShell script appears to be launching mimikatz, a password dumping utility. This is often launched as part of a PowerShell exploit kit. Decode and review the script.						
ACTION TAKEN	Process blocked						



CONVERSATIONAL LANGUAGE IN DOCS

Objective	Icon	Definition	Associated MITRE Tactics
Gain Access		Gaining access to your endpoints is a key phase in an adversary's attack strategy. A common way to get in is to steal credentials, using digital or social engineering methods.	Initial Access, Credential Access, Privilege Escalation
Keep Access		After an adversary finds a way into your environment, they work on how to keep access. Their goal is to maintain their foothold and evade detection, perhaps for long periods, before they follow through on plans to steal and break things in your environment.	Persistence, Defense Evasion
Explore		Once in, an adversary often explores the endpoint they gained access to and its connected systems. They'll poke around to discover local processes, files, and apps that could be useful to them.	Discover, Lateral Movement
Contact Controlled Systems		Command and control techniques use ports, proxies, and protocols that are native and approved, so it's challenging to detect suspicious and malicious use compared to harmless use.	Command and Control
Follow Through		Ultimately, an adversary is looking to steal and break things in your environment. They do this by gathering data, stealing data, and running malicious code.	Collection, Exfiltration, Execution





IT WORKED

Customers appreciate they can quickly explain detections to their team and management, regardless of security expertise



WHAT WE HEARD FROM CUSTOMERS

-
- “If you can’t explain something, you don’t know what it is. I feel with these new details, I can tell them XYZ happened, please check on this exact thing.”
 - “We find it useful for younger analysts as well”
 - “They aren’t a very technical crowd ... so it's like learning that there's this whole new language that's way easier to understand and act on.”
-





TRY THIS AT HOME

Worksheet and cheat sheet are in the deck

Thank you!





An adversary is trying to _____

ATT&CK tactic	Explain it to a non-security person
Initial Access	
Execution	
Persistence	
Privilege Escalation	
Defense Evasion	
Credential Access	
Discovery	
Lateral Movement	
Collection	
Exfiltration	
Command and Control	





An adversary is trying to _____

ATT&CK tactic	Explain it to a non-security person	Objective
Initial Access	Get into your environment	Gain access
Execution	Run malicious code	Follow through (steal/break)
Persistence	Maintain foothold	Keep access
Privilege Escalation	Gain higher level permissions	Gain (more) access
Defense Evasion	Avoid detection	Keep access
Credential Access	Steal logins and passwords	Gain access
Discovery	Figure out your environment	Explore
Lateral Movement	Move through your environment	Explore
Collection	Gather data	Follow through
Exfiltration	Steal data	Follow through
Command and Control	Contact controlled systems	Contact controlled systems

