Bijlage: Mapping misleidingstechnieken op de Unified Kill Chain / MITRE ATT&CK

Kill-chain fase	Through						Out	
ATT&CK tactiek	Discovery	Privilege Escalation	Execution	Credential Access	Lateral Movement	Collection	Exfiltration	Impact
ATT&CK techniek	Account Discovery	Abuse Elevation Control Mechanism	Cloud Administration Command	Adversary-in-the-Middle	Exploitation of Remote Services	Adversary-in-the-Middle	Automated Exfiltration	Account Access Removal
	Application Window Discovery	Access Token Manipulation	Command and Scripting Interpreter	Brute Force	Internal Spearphishing	Archive Collected Data	Data Transfer Size Limits	Data Destruction
	Browser Information Discovery	Account Manipulation	Container Administration Command	Credentials from Password Stores	Lateral Tool Transfer	Audio Capture	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
	Cloud Infrastructure Discovery	Boot or Logon Autostart Execution	Deploy Container	Exploitation for Credential Access	Remote Service Session Hijacking	Automated Collection	Exfiltration Over C2 Channel	Data Manipulation
	Cloud Service Dashboard	Boot or Logon Initialization Scripts	ESXi Administration Command	Forced Authentication	Remote Services	Browser Session Hijacking	Exfiltration Over Other Network Medium	Defacement
	Cloud Service Discovery	Create or Modify System Process	Exploitation for Client Execution	Forge Web Credentials	Replication Through Removable Media	Clipboard Data	Exfiltration Over Physical Medium	Disk Wipe
	Cloud Storage Object Discovery	Domain or Tenant Policy Modification	Input Injection	Input Capture	Software Deployment Tools	Data from Cloud Storage	Exfiltration Over Web Service	Email Bombing
	Container and Resource Discovery	Escape to Host	Inter-Process Communication	Modify Authentication Process	Taint Shared Content	Data from Configuration Repository	Scheduled Transfer	Endpoint Denial of Service
	Debugger Evasion	Event Triggered Execution	Native API	Multi-Factor Authentication Interception	Use Alternate Authentication Material	Data from Information Repositories	Transfer Data to Cloud Account	Financial Theft
	Device Driver Discovery	Exploitation for Privilege Escalation	Poisoned Pipeline Execution	Multi-Factor Authentication Request Generation		Data from Local System		Firmware Corruption
	Domain Trust Discovery	Hijack Execution Flow	Scheduled Task/Job	Network Sniffing		Data from Network Shared Drive		Inhibit System Recovery
	File and Directory Discovery	Process Injection	Serverless Execution	OS Credential Dumping		Data from Removable Media		Network Denial of Service
	Group Policy Discovery	Scheduled Task/Job	Shared Modules	Steal Application Access Token		Data Staged		Resource Hijacking
	Log Enumeration	Valid Accounts	Software Deployment Tools	Steal or Forge Authentication Certificates		Email Collection		Service Stop
	Network Service Discovery		System Services	Steal or Forge Kerberos Tickets		Input Capture		System Shutdown/Reboot
	Network Share Discovery		User Execution	Steal Web Session Cookie		Screen Capture		
	Network Sniffing		Windows Management Instrumentation	Unsecured Credentials		Video Capture		
	Password Policy Discovery							
	Peripheral Device Discovery							
	Permission Groups Discovery							
	Process Discovery							
	Query Registry							
	Remote System Discovery							
	Software Discovery							
	System Information Discovery							
	System Location Discovery							
	System Network Configuration Discovery							
	System Network Connections Discovery							
	System Owner/User Discovery							
	System Service Discovery							
	System Time Discovery							
	Virtual Machine Discovery							
	Virtualization/Sandbox Evasion							

Toelichting

Gebruik deze tabel om inzichtelijk te krijgen hoe jij misleiding kan gebruiken om deze aanvaller te detecteren.
Een aanvaller die toegang heeft verkregen tot jouw netwerk maakt gebruik van verschillende tactieken en technieken om zijn doelen te behalen.
In deze tabel vind je een overzicht van deze tactieken en technieken zoals gespecificeerd in de Unified Kill Chain en MITRE ATT&CK (klik op de technieken om hier meer over te leren).
Voor elk van deze technieken is aangegeven of jij een aanvaller die deze techniek gebruikt in de val kunt lokken en/of detecteren.
Lees ook ons artikel over dit onderwerp voor meer informatie: https://www.ncsc.nl/detectie/digitaal-struikeldraad/gerichte-misleiding

Legenda	
	Lokken
	Detecteren
	Lokken en/of detecteren