Bringing Intelligence into Cyber Deception with MITRE ATT&CK®

Adam Pennington

@_whatshisface

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD

Deception and Cyber Deception

Deception Planning & ATT&CK Basics

Intel-Driven Cyber Deception Planning

Takeaways

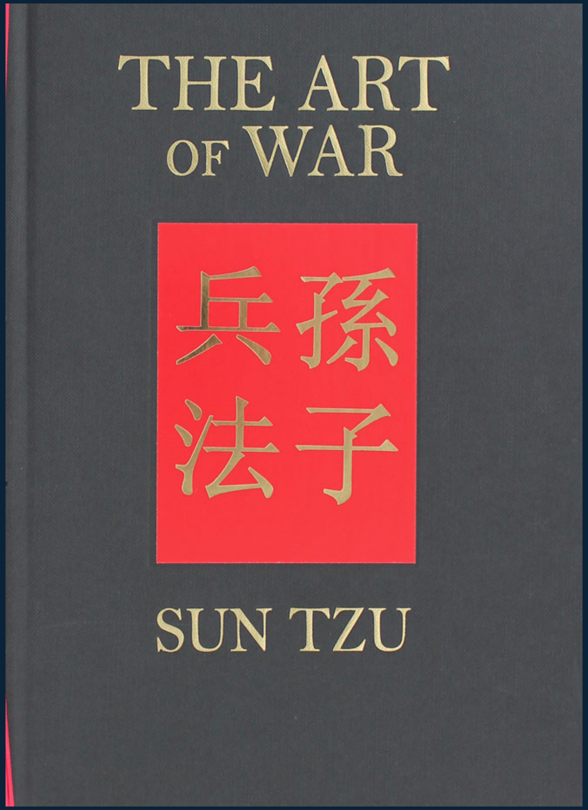
Deception

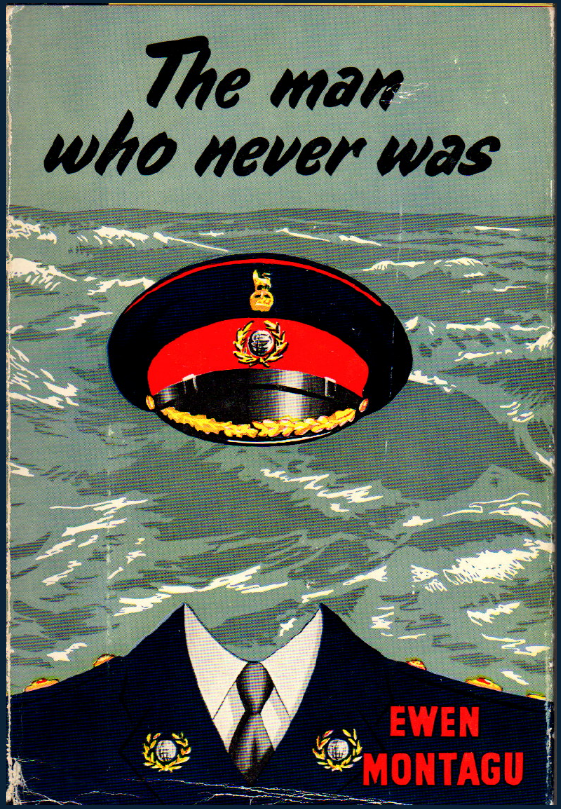
de·cep·tion | \ *di-ˈsep-shən* \

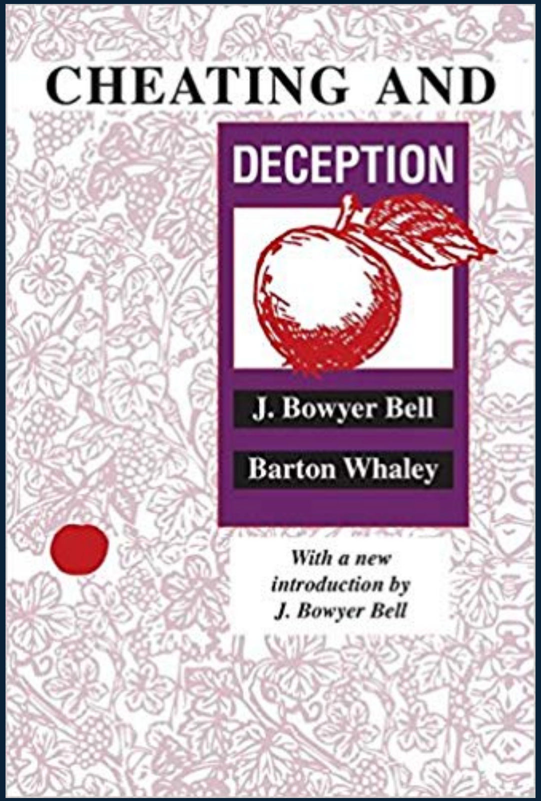
the act of causing someone to accept as true or valid what is false or invalid

- “Deception.” Merriam-Webster Dictionary

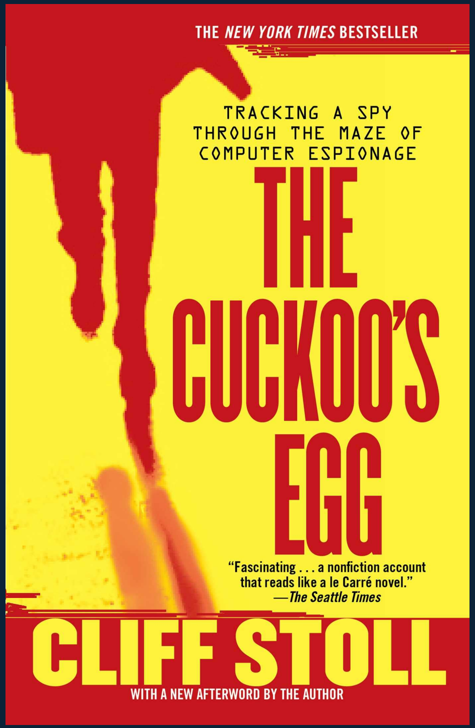
Deception and Warfare





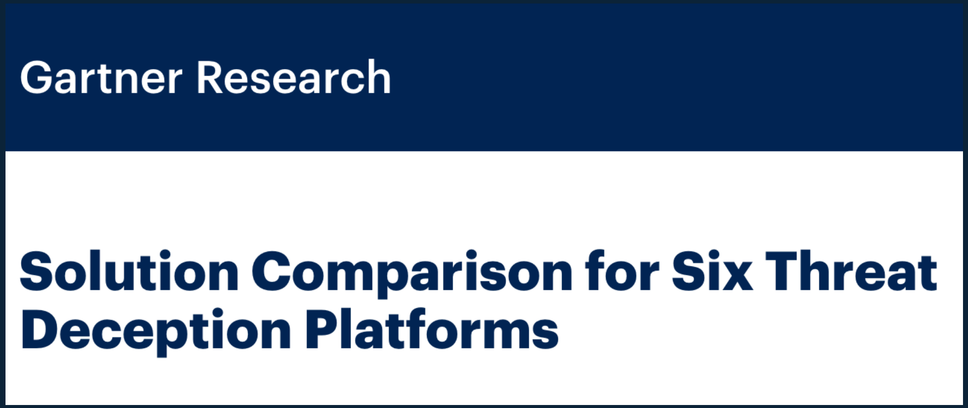


Cyber Deception Milestones


THE NEW YORK TIMES BESTSELLER
TRACKING A SPY THROUGH THE MAZE OF COMPUTER ESPIONAGE
THE CUCKOO'S EGG
"Fascinating . . . a nonfiction account that reads like a le Carré novel."
—The Seattle Times
CLIFF STOLL
WITH A NEW AFTERWORD BY THE AUTHOR

1989

1999



Gartner Research

Solution Comparison for Six Threat Deception Platforms

2019

Cyber Deception Goals

- **Deception for detection**
  - Honeypots
  - Honeytokens
- **Deception for intel gathering**
  - Honeypots
  - Honeynets
  - “Deception environments”

MITRE

Frequent Cyber Deception Problems

- **Mismatched Visibility**
  - Capabilities not where adversaries are looking
  - Capability: Can only be found via port scanning
  - Adversary: Looks for targets via Active Directory
- **Mismatched expectations**
  - Capabilities don’t look like what adversaries expect
  - Capability: Single local account whose password just changed
  - Adversary: Looks for many well-established domain accounts

We know how to do deception, what’s going wrong?

Mirror Imaging: Deception's Enemy

To say, "if I were a Russian intelligence officer . . ." or "if I were running the Indian Government . . ." is mirror-imaging. Analysts may have to do that when they do not know how the Russian intelligence officer or the Indian Government is really thinking. But **mirror-imaging leads to dangerous assumptions, because people in other cultures do not think the way we do.**

-Richards Heuer

Photo by ŠJů is licensed under CC BY-SA

Learning From our Past: Deception Planning

1. **Research adversary**
   - Know adversary's preconceptions, expectations, & reactions
2. **Design deception**
   - Develop cover story
   - Determine what must be hidden and what needs to be created
   - Hide the real: plan steps to mask, repackage, dazzle, or red flag
   - Show the false: plan steps to mimic, invent, decoy, or double play
   - Develop deception plan: organize the necessary D&D means/resources
3. **Deploy deception**
4. **Monitor and control**
   - Observation channels and sources
   - Adversary reactions

Adapted from Barton Whaley's "General Theory of Deception" by Frank Stech and Kristen Heckman

Applying Traditional Deception to Cyber Deception

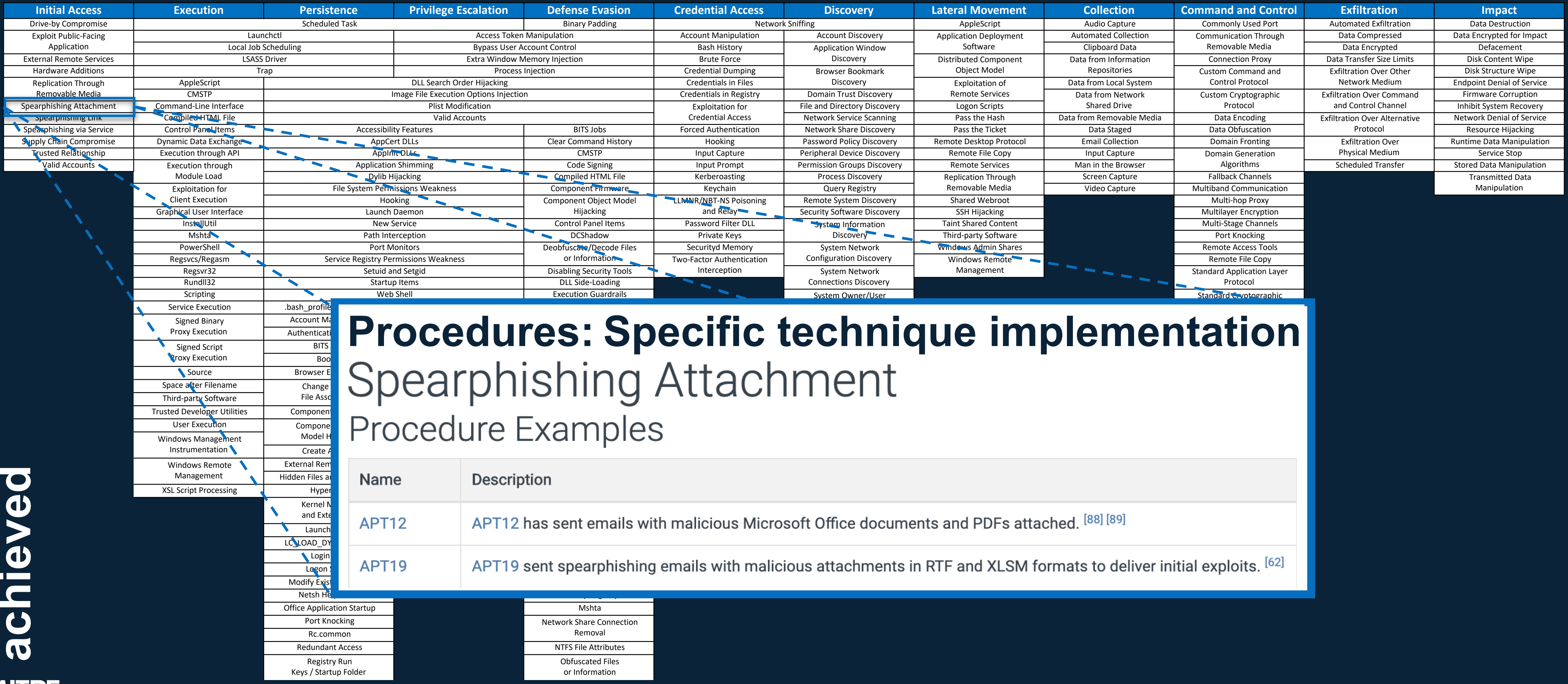
- **Traditional deception planning is an intel-driven process**
  - We can apply a similar process to cyber deception
- **Likely won’t know** preconceptions & expectations **directly**
  - Can infer based on behavior

- **Need to build intel and knowledge of how adversaries behave**
  - Enter ATT&CK

ATT&CK Knowledge Base Basics

Tactics: the adversary's technical goals

Techniques: how the goals are achieved



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	Scheduled Task			Binary Padding	Network Sniffing		AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	Launchctl		Access Token Manipulation		Account Manipulation	Account Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
	Local Job Scheduling		Bypass User Account Control		Bash History	Application Window Discovery		Clipboard Data		Data Encrypted	Defacement
External Remote Services	LSASS Driver		Extra Window Memory Injection		Brute Force		Distributed Component Object Model	Data from Information Repositories	Connection Proxy	Data Transfer Size Limits	Disk Content Wipe
Hardware Additions	Trap		Process Injection		Credential Dumping	Browser Bookmark Discovery			Custom Command and Control Protocol	Exfiltration Over Other Network Medium	Disk Structure Wipe
Replication Through Removable Media	AppleScript	DLL Search Order Hijacking			Credentials in Files		Exploitation of Remote Services	Data from Local System			Endpoint Denial of Service
	CMSTP	Image File Execution Options Injection			Credentials in Registry	Domain Trust Discovery		Data from Network Shared Drive	Custom Cryptographic Protocol	Exfiltration Over Command and Control Channel	Firmware Corruption
Spearphishing Attachment	Command-Line Interface	Plist Modification			Exploitation for Credential Access	File and Directory Discovery	Logon Scripts				Inhibit System Recovery
Spearphishing Link	Compiled HTML File	Valid Accounts				Network Service Scanning	Pass the Hash	Data from Removable Media	Data Encoding	Exfiltration Over Alternative Protocol	Network Denial of Service
Spearphishing via Service	Control Panel Items	Accessibility Features		BITS Jobs	Forced Authentication	Network Share Discovery	Pass the Ticket	Data Staged	Data Obfuscation		Resource Hijacking
Supply Chain Compromise	Dynamic Data Exchange	AppCert DLLs		Clear Command History	Hooking	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Fronting	Exfiltration Over Physical Medium	Runtime Data Manipulation
Trusted Relationship	Execution through API	AppInit DLLs		CMSTP	Input Capture	Peripheral Device Discovery	Remote File Copy	Input Capture	Domain Generation Algorithms		Service Stop
Valid Accounts	Execution through Module Load	Application Shimming		Code Signing	Input Prompt	Permission Groups Discovery	Remote Services	Man in the Browser		Scheduled Transfer	Stored Data Manipulation
		Dylib Hijacking		Compiled HTML File	Kerberoasting	Process Discovery	Replication Through Removable Media	Screen Capture	Fallback Channels		Transmitted Data Manipulation
	Exploitation for Client Execution	File System Permissions Weakness		Component Firmware	Keychain	Query Registry		Video Capture	Multiband Communication		
		Hooking		Component Object Model Hijacking	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Shared Webroot		Multi-hop Proxy		
	Graphical User Interface	Launch Daemon				Security Software Discovery	SSH Hijacking		Multilayer Encryption		
	InstallUtil	New Service		Control Panel Items	Password Filter DLL	System Information Discovery	Taint Shared Content		Multi-Stage Channels		
	Mshta	Path Interception		DCShadow	Private Keys		Third-party Software		Port Knocking		
	PowerShell	Port Monitors		Deobfuscate/Decode Files or Information	Securityd Memory	System Network Configuration Discovery	Windows Admin Shares		Remote Access Tools		
	Regsvcs/Regasm	Service Registry Permissions Weakness			Two-Factor Authentication Interception		Windows Remote Management		Remote File Copy		
	Regsvr32	Setuid and Setgid		Disabling Security Tools		System Network Connections Discovery			Standard Application Layer Protocol		
	Rundll32	Startup Items		DLL Side-Loading							
	Scripting	Web Shell		Execution Guardrails		System Owner/User			Standard Cryptographic		
	Service Execution	.bash_profile									
	Signed Binary Proxy Execution	Account Ma									
		Authenticati									
	Signed Script Proxy Execution	BITS									
		Boo									
	Source	Browser E									
	Space after Filename	Change File Ass									
	Third-party Software										
	Trusted Developer Utilities	Component									
	User Execution	Compone Model H									
	Windows Management Instrumentation										
		Create A									
	Windows Remote Management	External Rem									
		Hidden Files ar									
	XSL Script Processing	Hyper									
		Kernel M and Exte									
		Launch									
		LC_LOAD_DY									
		Login									
		Logon S									
		Modify Exis									
		Netsh He									
		Office Application Startup		Mshta							
		Port Knocking		Network Share Connection Removal							
		Rc.common									
		Redundant Access		NTFS File Attributes							
		Registry Run Keys / Startup Folder		Obfuscated Files or Information							

Procedures: Specific technique implementation

Spearphishing Attachment

Procedure Examples

Name	Description
APT12	APT12 has sent emails with malicious Microsoft Office documents and PDFs attached. [88] [89]
APT19	APT19 sent spearphishing emails with malicious attachments in RTF and XLSM formats to deliver initial exploits. [62]

MITRE

Cyber Deception Planning

Intel-Driven Cyber Deception Planning Process

0. Determine who your priority adversary(ies) are
1. Build adversary profile based on CTI
2. Develop a cover story
3. Determine what true info needs to be hidden/false info revealed for cover
4. Design & build the technical capability aligned with intel
5. Deploy the deception
6. Gather intelligence

0. Determine Who Your Priority Adversary(ies) Are

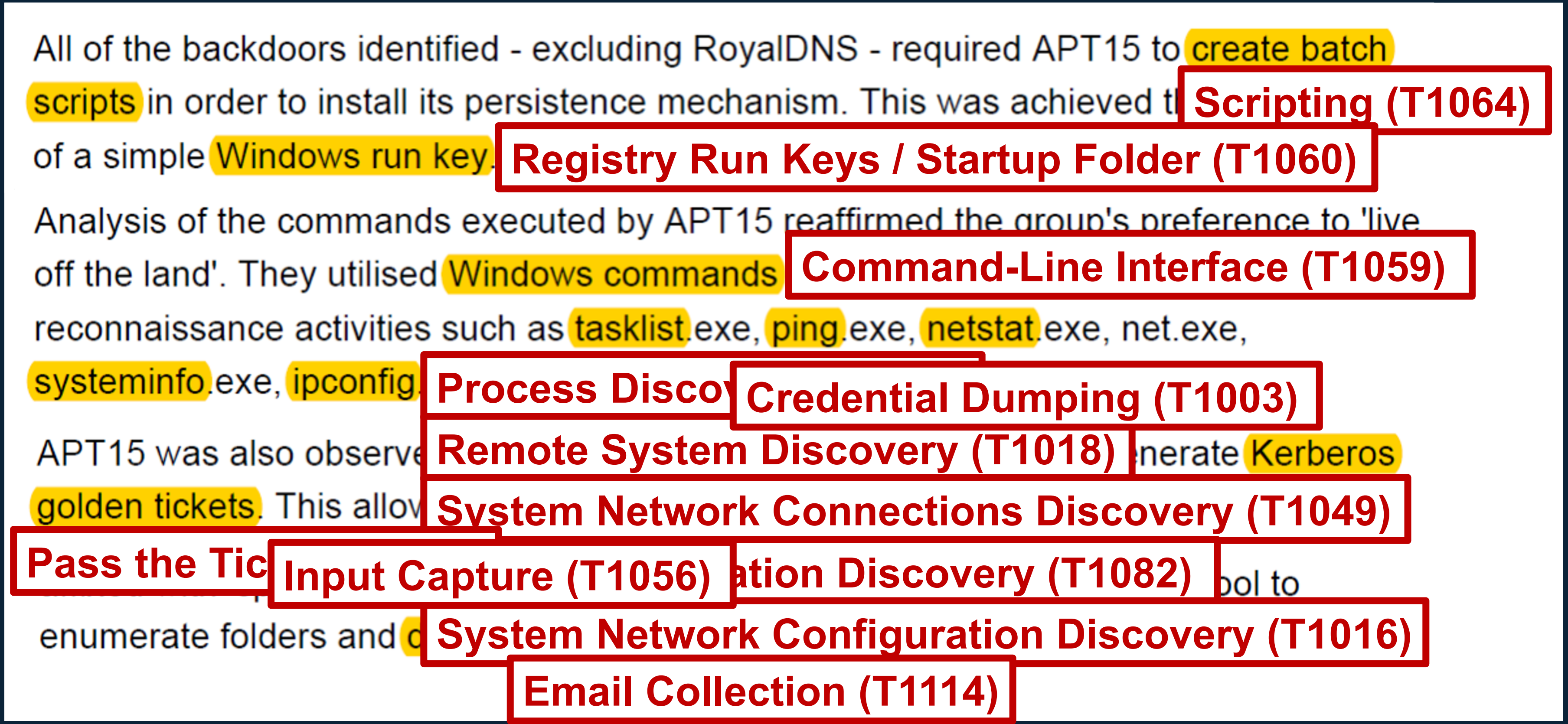
- Many ways to prioritize

- Adversary who targets you regularly
- Adversary who has targeted others like you
- Adversary who is likely to evade current defenses
- Adversary who little is currently known about (intel gap)

1. Build Adversary Profile Based on CTI

- Build up ATT&CK techniques used by adversary
- Can leverage the information in ATT&CK's groups/software
  - https://attack.mitre.org/groups/
- Open source reporting
- Commercial threat intelligence providers
- Supplement with your own CTI

Mapping ATT&CK Techniques



All of the backdoors identified - excluding RoyalDNS - required APT15 to create batch scripts in order to install its persistence mechanism. This was achieved tl

of a simple Windows run key.

Analysis of the commands executed by APT15 reaffirmed the group's preference to 'live off the land'. They utilised Windows commands

reconnaissance activities such as tasklist.exe, ping.exe, netstat.exe, net.exe,

systeminfo.exe, ipconfig.

APT15 was also observe nerate Kerberos

golden tickets. This allov

ool to

enumerate folders and c

Scripting (T1064)

Registry Run Keys / Startup Folder (T1060)

Command-Line Interface (T1059)

Process Discov

Credential Dumping (T1003)

Remote System Discovery (T1018)

System Network Connections Discovery (T1049)

Pass the Tic

Input Capture (T1056)

ation Discovery (T1082)

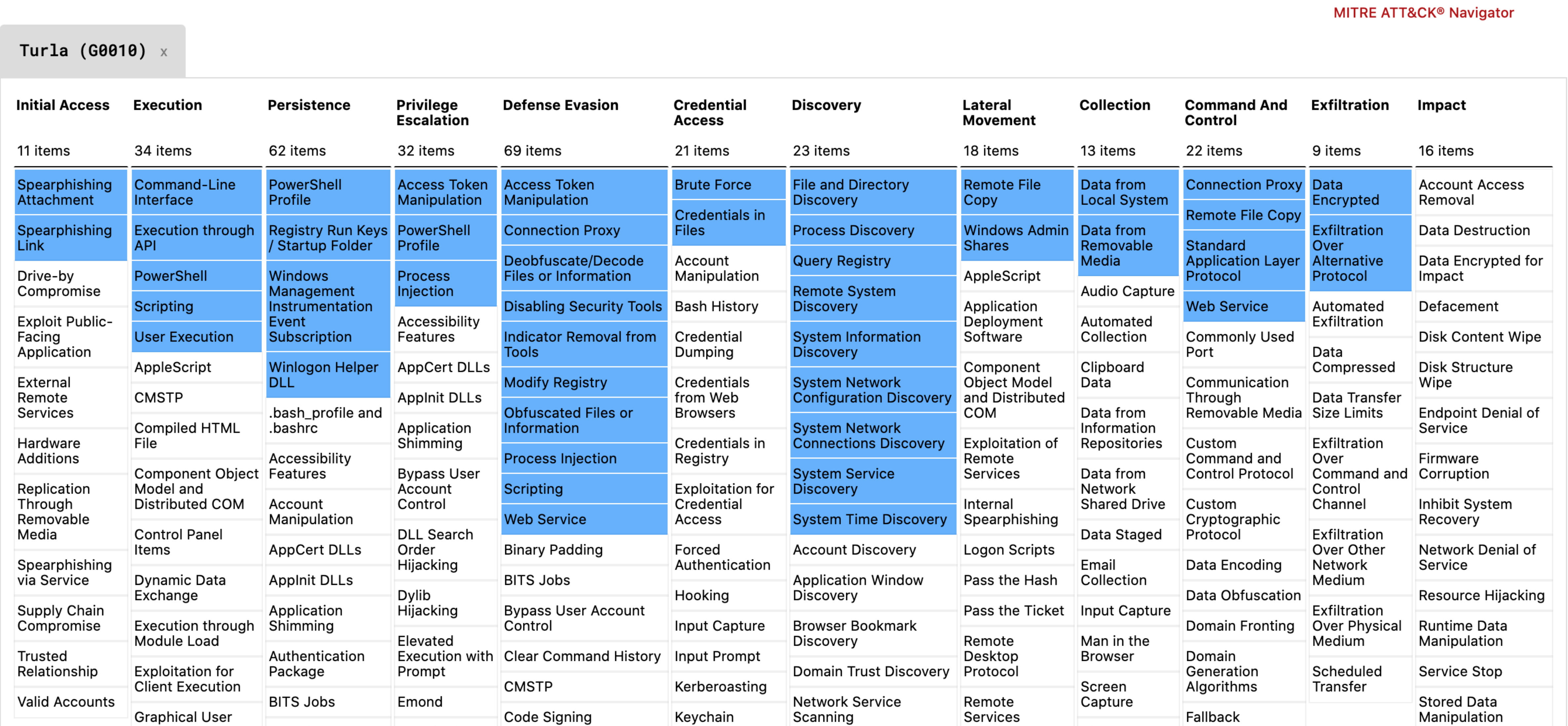
System Network Configuration Discovery (T1016)

Email Collection (T1114)

https://www.nccgroup.trust/us/about-us/newsroom-and-events/blog/2018/march/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/

Free training on using ATT&CK for CTI https://attack.mitre.org/resources/training/cti/

Example: Techniques Associated with Turla in ATT&CK



MITRE ATT&CK® Navigator

Turla (G0010) x

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	22 items	9 items	16 items
Spearphishing Attachment	Command-Line Interface	PowerShell Profile	Access Token Manipulation	Access Token Manipulation	Brute Force	File and Directory Discovery	Remote File Copy	Data from Local System	Connection Proxy	Data Encrypted	Account Access Removal
Spearphishing Link	Execution through API	Registry Run Keys / Startup Folder	PowerShell Profile	Connection Proxy	Credentials in Files	Process Discovery	Windows Admin Shares	Data from Removable Media	Remote File Copy	Exfiltration Over Alternative Protocol	Data Destruction
Drive-by Compromise	PowerShell	Windows Management Instrumentation Event Subscription	Process Injection	Deobfuscate/Decode Files or Information	Account Manipulation	Query Registry	AppleScript	Audio Capture	Standard Application Layer Protocol	Automated Exfiltration	Data Encrypted for Impact
Exploit Public-Facing Application	Scripting	Winlogon Helper DLL	Accessibility Features	Disabling Security Tools	Bash History	Remote System Discovery	Application Deployment Software	Automated Collection	Web Service	Data Compressed	Defacement
External Remote Services	User Execution	.bash_profile and .bashrc	AppCert DLLs	Indicator Removal from Tools	Credential Dumping	System Information Discovery	Component Object Model and Distributed COM	Clipboard Data	Commonly Used Port	Data Transfer Size Limits	Disk Content Wipe
Hardware Additions	AppleScript	Accessibility Features	AppInit DLLs	Modify Registry	Credentials from Web Browsers	System Network Configuration Discovery	Exploitation of Remote Services	Data from Information Repositories	Communication Through Removable Media	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Replication Through Removable Media	CMSTP	Account Manipulation	Application Shimming	Obfuscated Files or Information	Credentials in Registry	System Network Connections Discovery	Internal Spearphishing	Data from Network Shared Drive	Custom Command and Control Protocol	Exfiltration Over Network Medium	Endpoint Denial of Service
Spearphishing via Service	Compiled HTML File	AppCert DLLs	Bypass User Account Control	Process Injection	Exploitation for Credential Access	System Service Discovery	Logon Scripts	Data Staged	Custom Cryptographic Protocol	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Component Object Model and Distributed COM	AppInit DLLs	DLL Search Order Hijacking	Scripting	Forced Authentication	System Time Discovery	Pass the Hash	Email Collection	Data Encoding	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Control Panel Items	Application Shimming	Dylib Hijacking	Web Service	Hooking	Account Discovery	Pass the Ticket	Input Capture	Data Obfuscation		Network Denial of Service
Valid Accounts	Dynamic Data Exchange	Authentication Package	Elevated Execution with Prompt	Binary Padding	Input Capture	Application Window Discovery	Remote Desktop Protocol	Man in the Browser	Domain Fronting		Resource Hijacking
	Execution through Module Load	BITS Jobs	Emond	BITS Jobs	Input Prompt	Browser Bookmark Discovery	Remote Services	Screen Capture	Domain Generation Algorithms		Runtime Data Manipulation
	Exploitation for Client Execution			Bypass User Account Control	Kerberoasting	Domain Trust Discovery			Fallback		Service Stop
	Graphical User			Clear Command History	Keychain	Network Service Scanning					Stored Data Manipulation
				CMSTP							
				Code Signing							

MITRE

Techniques to Preconceptions and Expectations

- **We can infer what an adversary may expect based on technique use**
  - Introduces risk of bias, but direct intel unlikely
- **Example: Adversary uses Browser Bookmark Discovery (T1217)**
  - Inference: The adversary expects a browser
  - Inference: The adversary expects that browser has bookmarks
  - Inference: The adversary expects an interactive user

- **Example: Adversary uses Virtualization/Sandbox Evasion (T1497)**
  - Inference: The adversary expects not to be in a VM
  - Inference: The adversary believes that a VM may be bad

2. Develop a Cover Story

- **What the target of the deception should perceive and believe**
  - “Generally, the most convincing cover stories are based on what the opponent already believes and wants to believe.” -Heckman et al.

- **What does the adversary expect?**
  - Leverage the intelligence we’ve been building
- **Are there limitations we need to account for?**
  - Example: Our budget is limited so we can only afford a few systems

Turla Initial Access Techniques from ATT&CK

Initial Access	
Drive-by Compromise	Spearphishing Attachment
Exploit Public-Facing	Spearphishing Link
Application	Spearphishing via Service
External Remote Services	Supply Chain Compromise
Hardware Additions	Trusted Relationship
Replication Through	Valid Accounts
Removable Media	Spearphishing Attachment

- **Can infer Turla is expecting email and end user systems**

Turla Discovery Techniques from ATT&CK

Discovery	
Account Discovery	Process Discovery
Application Window Discovery	Query Registry
Browser Bookmark Discovery	Remote System Discovery
Domain Trust Discovery	Security Software Discovery
File and Directory Discovery	System Information Discovery
Network Service Scanning	System Network Configuration Discovery
Network Share Discovery	System Network Connections Discovery
Network Sniffing	System Owner/User Discovery
Password Policy Discovery	System Service Discovery
Peripheral Device Discovery	System Time Discovery
Permission Groups Discovery	Virtualization/Sandbox Evasion

- **Can infer Turla is expecting multiple systems**

Example Cover Story – ACME Corp

- Is a small subsidiary of existing company located in Zurich, Switzerland
- Has a dozen users, each with their own Windows desktop on a domain
- Has its own email and file servers
- …

- Accounts for limited budget (small number of systems/users)
- Meets expectations of multiple systems, email, and end user systems

3. Determine What Info Needs to be Hidden/Revealed

Danita Delimont Creative / Alamy Stock Photo

D&D Methods Matrix with Cyber D&D Techniques

Deception Objects	Deception: Revealing	Denial: Concealing
Facts	**Reveal facts:** • Use true network info • Allow disclosure of real file • Selectively remediate	**Conceal facts:** • Hide collection software • Deny access to resources
Fictions	**Reveal fictions:** • Misrepresent intent of sw • Expose fictional systems • Disclose fictional info	**Conceal Fictions:** • Hide simulated info • OPSEC around deception • Only allow partial enumeration of fake files

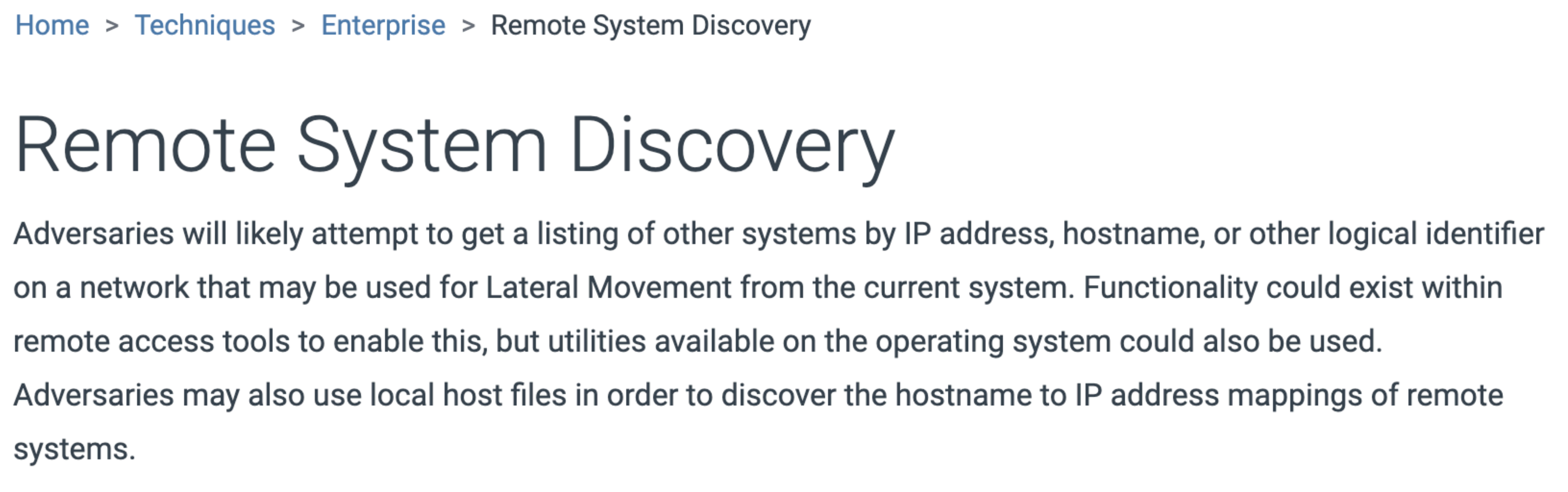
From Cyber Denial, Deception, & Counterdeception by Heckman et al.

Turla Discovery Techniques from ATT&CK

Discovery	
Account Discovery	Process Discovery
Application Window Discovery	Query Registry
Browser Bookmark Discovery	Remote System Discovery
Domain Trust Discovery	Security Software Discovery
File and Directory Discovery	System Information Discovery
Network Service Scanning	System Network Configuration Discovery
Network Share Discovery	System Network Connections Discovery
Network Sniffing	System Owner/User Discovery
Password Policy Discovery	System Service Discovery
Peripheral Device Discovery	System Time Discovery
Permission Groups Discovery	Virtualization/Sandbox Evasion

MITRE

T1018 - Remote System Discovery



Home > Techniques > Enterprise > Remote System Discovery

Remote System Discovery

Adversaries will likely attempt to get a listing of other systems by IP address, hostname, or other logical identifier on a network that may be used for Lateral Movement from the current system. Functionality could exist within remote access tools to enable this, but utilities available on the operating system could also be used. Adversaries may also use local host files in order to discover the hostname to IP address mappings of remote systems.

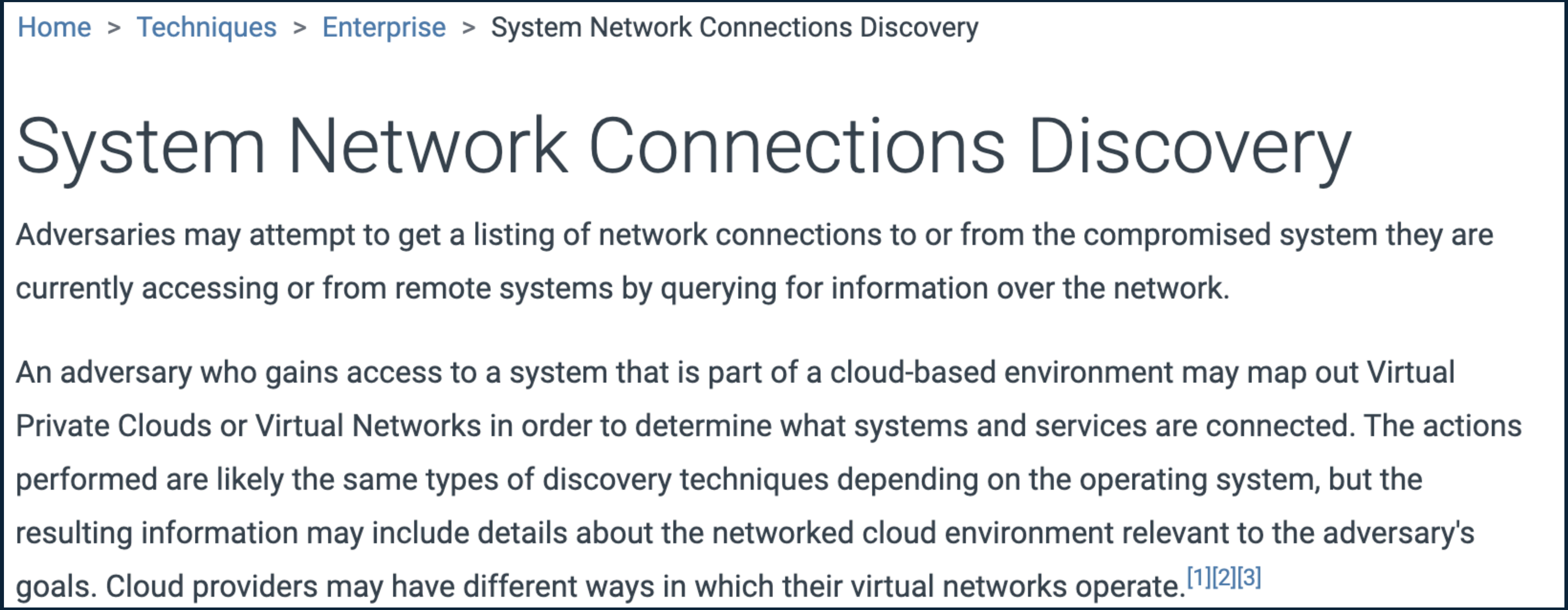
- **Reveal Fiction** – Expose fake remote systems on network
- **Conceal Fact** – Hide collection system from T1018

MITRE

Turla Discovery Techniques from ATT&CK

Discovery	
Account Discovery	Process Discovery
Application Window Discovery	Query Registry
Browser Bookmark Discovery	Remote System Discovery
Domain Trust Discovery	Security Software Discovery
File and Directory Discovery	System Information Discovery
Network Service Scanning	System Network Configuration Discovery
Network Share Discovery	System Network Connections Discovery
Network Sniffing	System Owner/User Discovery
Password Policy Discovery	System Service Discovery
Peripheral Device Discovery	System Time Discovery
Permission Groups Discovery	Virtualization/Sandbox Evasion

T1049 – System Network Connections Discovery



Home > Techniques > Enterprise > System Network Connections Discovery

System Network Connections Discovery

Adversaries may attempt to get a listing of network connections to or from the compromised system they are currently accessing or from remote systems by querying for information over the network.

An adversary who gains access to a system that is part of a cloud-based environment may map out Virtual Private Clouds or Virtual Networks in order to determine what systems and services are connected. The actions performed are likely the same types of discovery techniques depending on the operating system, but the resulting information may include details about the networked cloud environment relevant to the adversary's goals. Cloud providers may have different ways in which their virtual networks operate.[1][2][3]

- **Reveal Fiction** – Create connections to target host
- **Conceal Fact** – Hide connection to logging system

MITRE

Augmented Cyber D&D Method Matrix

Deception Objects	Deception: Revealing	Denial: Concealing
Facts	**Reveal facts:** • Use true network info • Allow disclosure of real file • Selectively remediate	**Conceal facts:** • Hide collection software • Deny access to resources • Hide connection to logging • Hide collection system
Fictions	**Reveal fictions:** • Misrepresent intent of sw • Expose fictional systems • Disclose fictional info • Connections to target host • Expose fake remote sys	**Conceal Fictions:** • Hide simulated info • OPSEC around deception • Only allow partial enumeration of fake files

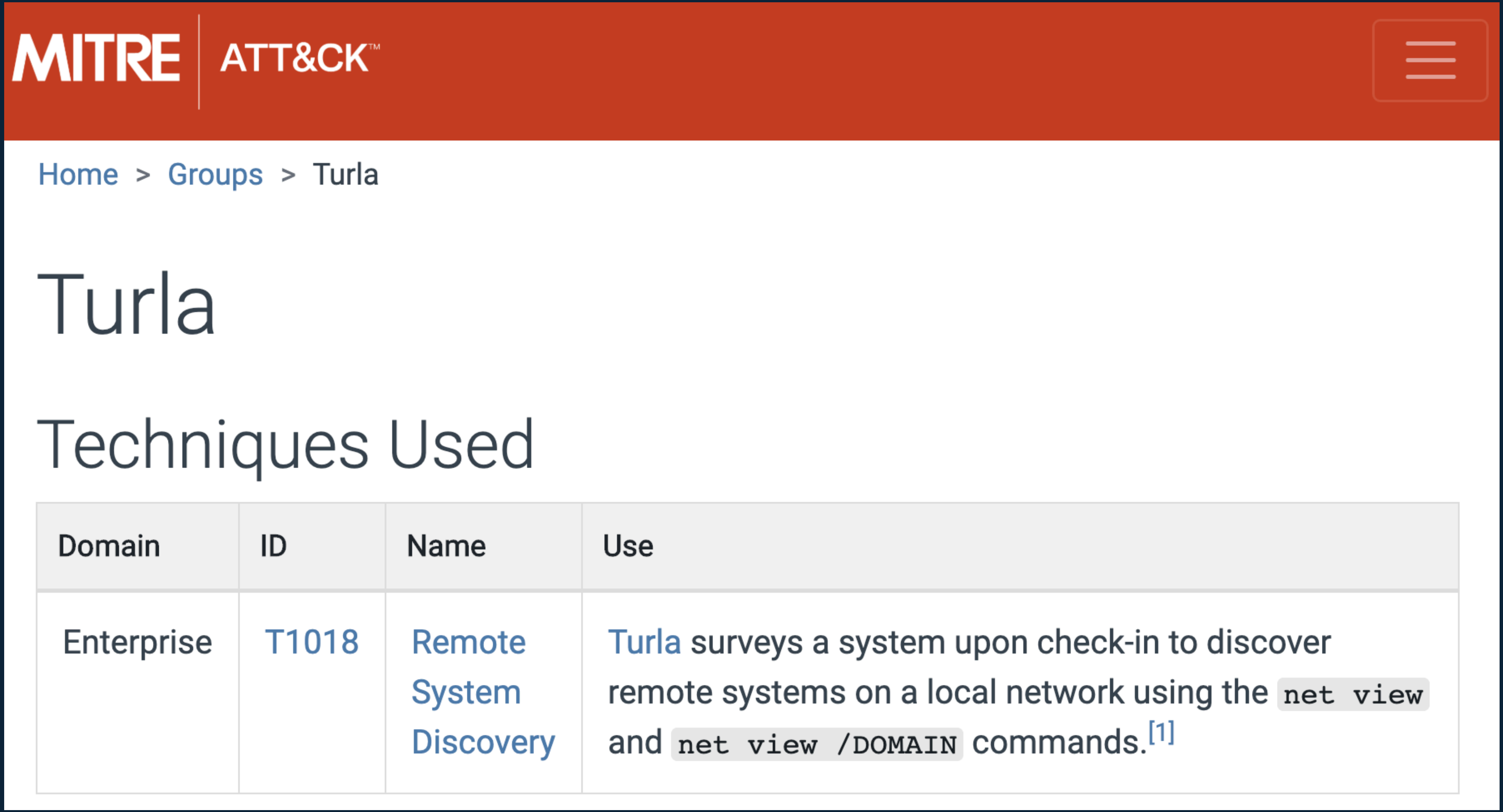
From Cyber Denial, Deception, & Counterdeception by Heckman et al.

MITRE

4. Design & Build the Technical Capability

- **Implement the D&D matrix in line with cover story**
  - Design and build revealed facts and fictions
  - Design and build concealment around denied facts and fictions
- **Leverage details of technique use (procedures)**
  - Further meet adversary expectations

Turla’s use of Remote System Discovery



Home > Groups > Turla

Turla

Techniques Used

Domain	ID	Name	Use
Enterprise	T1018	Remote System Discovery	Turla surveys a system upon check-in to discover remote systems on a local network using the `net view` and `net view /DOMAIN` commands.[1]

Matching Visibility and Expectations

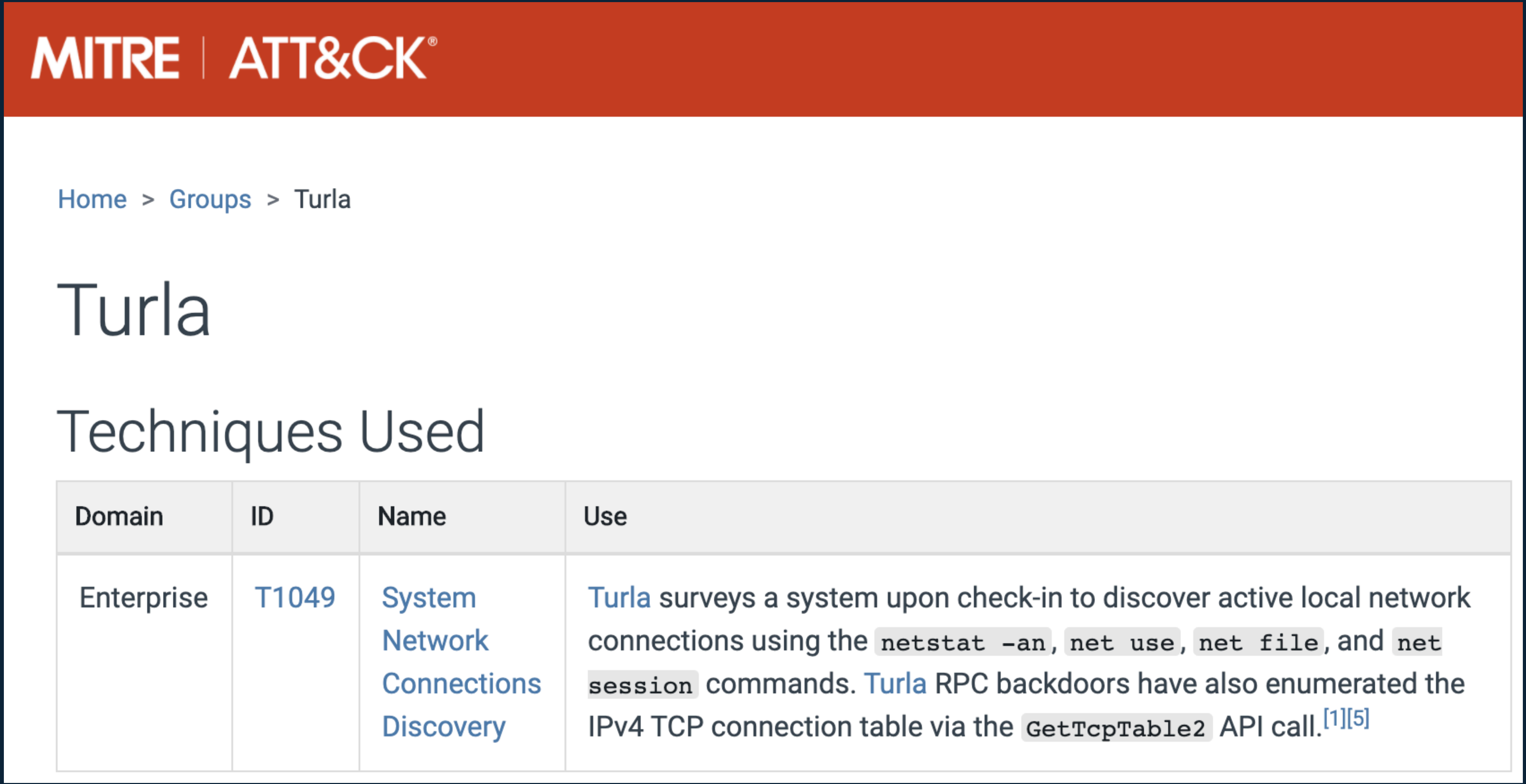
Reveal Fiction – Expose fake remote systems on network

- **Turla appears to expect `net view` & `net view /DOMAIN` to work**

Design Decisions

- **Place fake Windows system on the network**
- **Make sure fake system shows up in computer browsing**
  - Services likely will need to be enabled in fresh setup

Turla’s use of System Network Connections Discovery



Home > Groups > Turla

Turla

Techniques Used

Domain	ID	Name	Use
Enterprise	T1049	System Network Connections Discovery	Turla surveys a system upon check-in to discover active local network connections using the `netstat -an`, `net use`, `net file`, and `net session` commands. Turla RPC backdoors have also enumerated the IPv4 TCP connection table via the `GetTcpTable2` API call.[1][5]

Matching Visibility and Expectations

Reveal Fiction – Create connections to target host

Conceal Fact – Hide connection to logging system

- Turla appears to expect `netstat -an`, `net use`, `net file`, `net session`, or `GetTcpTable2` to work

Design Decisions

- Create standing connections with `net use`
- Leverage UDP for logging

MITRE

5. Deploy the Deception

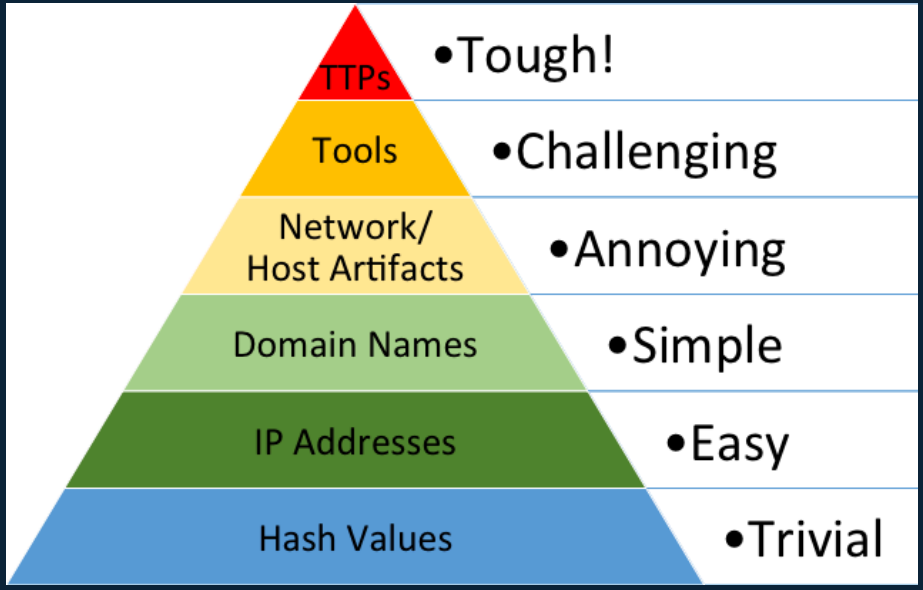
- **Deception for detection**
  - – Deploy/turn on and wait for an alert
- **Deception for intel gathering**
  - – Wait for an opportunity

MITRE

6. Gather Intelligence

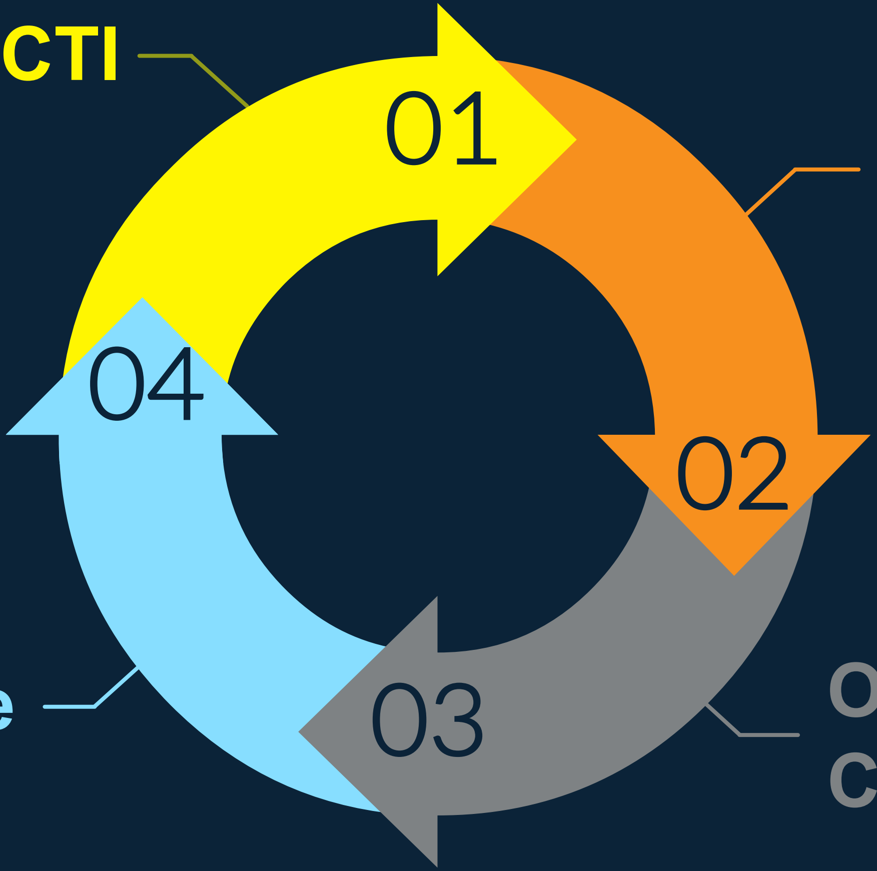
- Many possible types of intelligence

- Adversary presence
  - Detection and alerting capability
- Techniques used by adversaries
  - Host/network monitoring
  - Command and control decoding
- Indicators of compromise
  - Files/IPs/hostnames etc used by adversaries



Source: David Bianco, https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Leverage Intelligence and Iterate



Build Profile from CTI

Design & Deploy Deception

Operate Deception Capability

Gather Intelligence

Intel-driven Cyber Deception Planning

0. Determine who your priority adversary(ies) are
1. Build adversary profile based on CTI
2. Develop a cover story
3. Determine what true info needs to be hidden/false info revealed for cover
4. Design & build the technical capability aligned with intel
5. Deploy the deception
6. Gather intelligence

Takeaways

We can apply practices from historical deception planning to cyber deception

Cyber threat intelligence can play a critical role throughout cyber deception

Adversary behaviors/ATT&CK techniques have uses beyond "traditional" defensive practices

ATT&CK

https://attack.mitre.org

attack@mitre.org

Adam Pennington

🐦@_whatshisface

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD

References

Heckman, K. et al., “Cyber Denial, Deception, & Counter Deception”

Heuer, R., “Psychology of Intelligence Analysis”

Whaley, B., “Toward a general theory of deception”

https://attack.mitre.org/