Why Should Blue Team Love MITRE ATT&CK (Adversary, Technique, Tactic & Common Knowledge)

Digit Oktavianto
Independent Security Researcher

CDEF 8th Meetup

Telkomsel – 11th July 2019

Who Am I

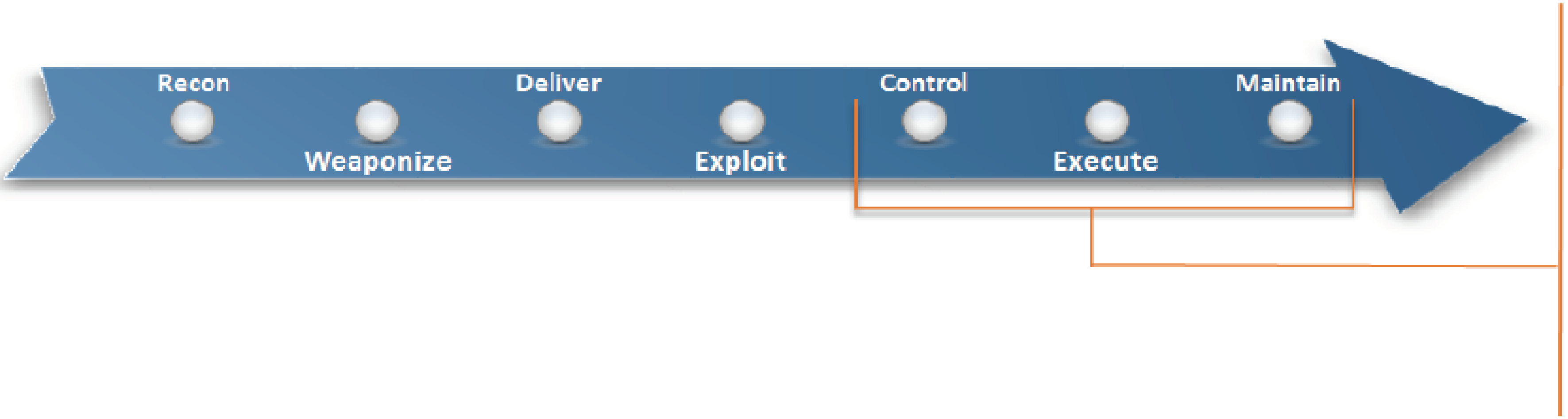
- Infosec Consulting Manager at MII
- Born to be DFIR Team
- Tim Hore Cyber Defense Community Indonesia
- Member Indonesia Honeynet Project
- Member Asosiasi Cloud Computing Indonesia
- Opreker and Researcher

MITRE ATT&CK Framework

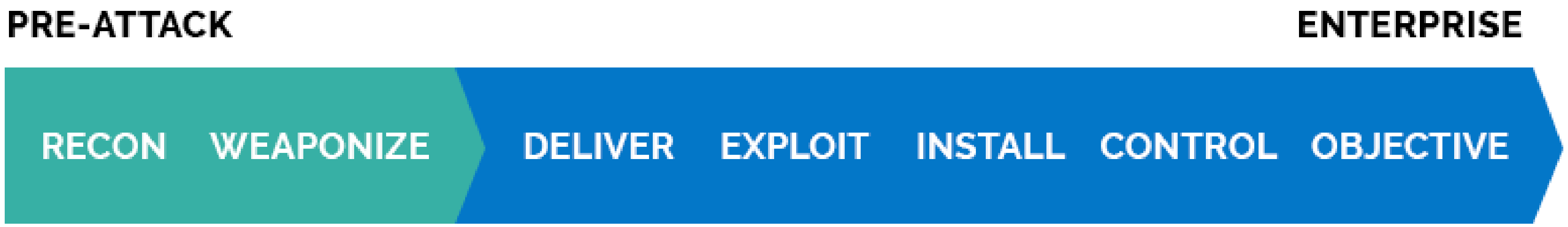
- MITRE ATT&CK™ is a globally-accessible knowledge base of **adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies** in the private sector, in government, and in the cybersecurity product and service community.

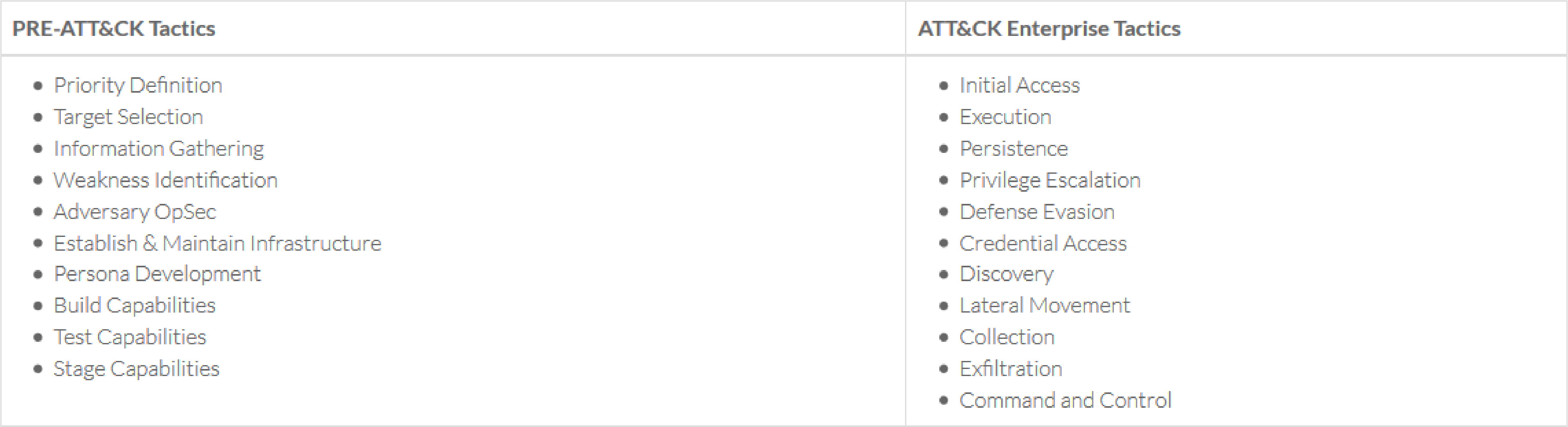
  With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge

Cyber Kill Chain VS MITRE ATT&CK Framework



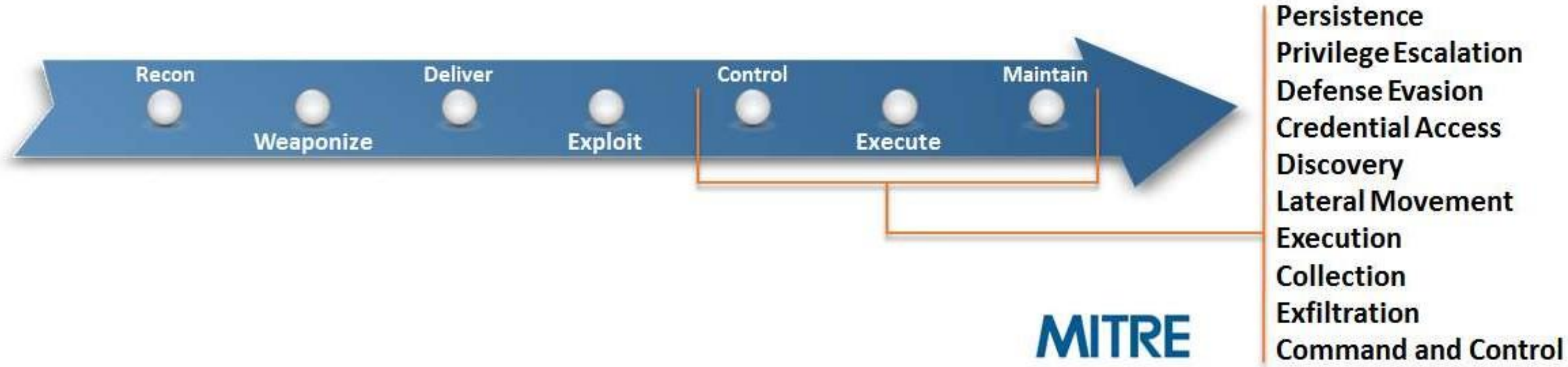
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Execution
Collection
Exfiltration
Command and Control





PRE-ATT&CK Tactics	ATT&CK Enterprise Tactics
• Priority Definition • Target Selection • Information Gathering • Weakness Identification • Adversary OpSec • Establish & Maintain Infrastructure • Persona Development • Build Capabilities • Test Capabilities • Stage Capabilities	• Initial Access • Execution • Persistence • Privilege Escalation • Defense Evasion • Credential Access • Discovery • Lateral Movement • Collection • Exfiltration • Command and Control

Using MITRE ATT&CK Model



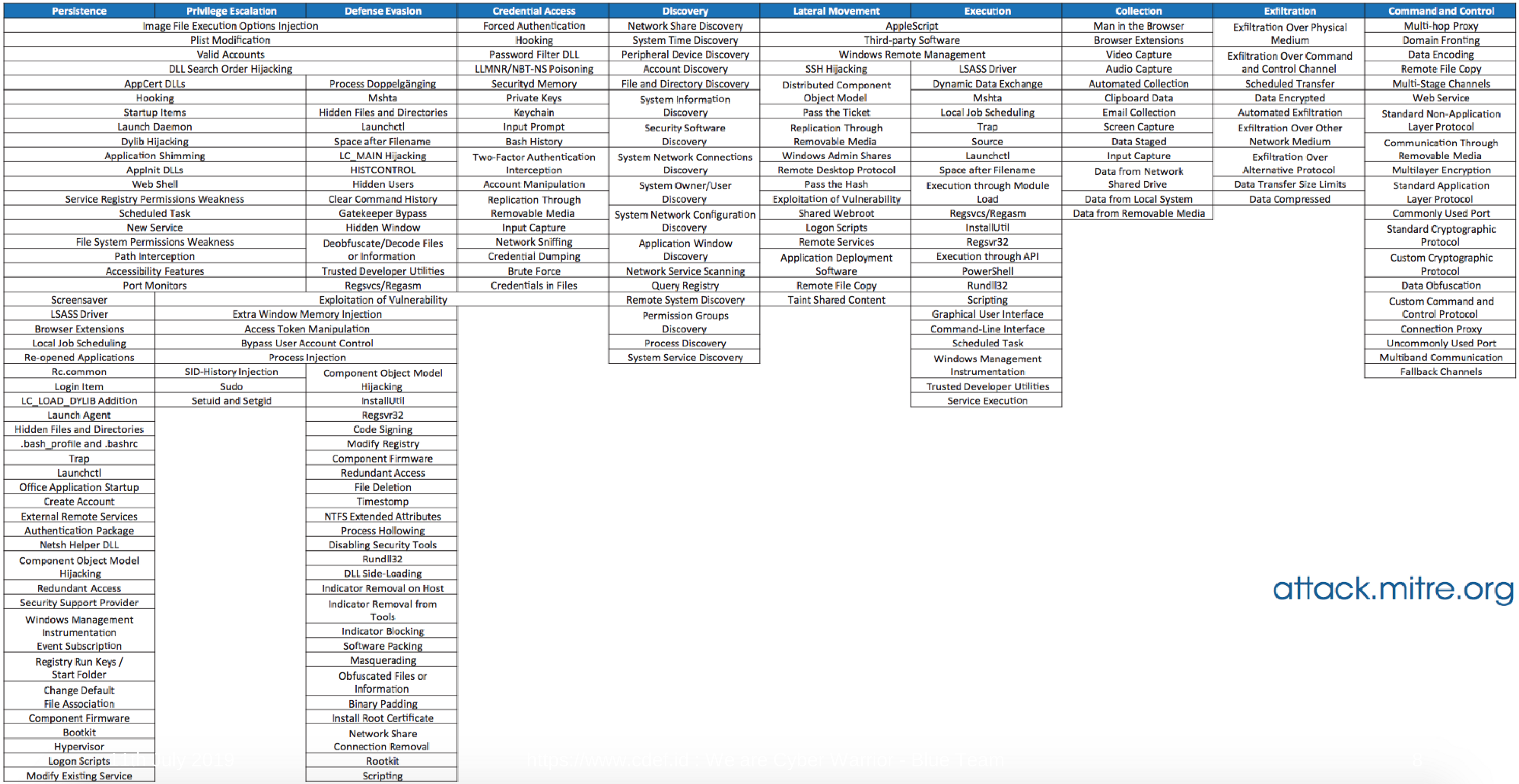
Used to characterize and describe post-compromise adversary behavior.

Details the post-compromise tactics, techniques, and procedures (TTPs) persistent threats use to execute their objectives while operating inside a network.

MITRE ATT&CK Framework

- For example, the later stages (Control, Maintain, and Execute) of MITRE’s seven-stage ATT&CK lifecycle include categories like lateral movement and data exfiltration, under which many kinds of activities can exist. **Here’s an example list of potential attacker activities and techniques you might identify**:
- Malware Beaconing
- DLL Injection
- Pass the Hash (PtH)
- Mimikatz
- DNS Tunneling

MITRE Enterprise ATT&CK™ Framework

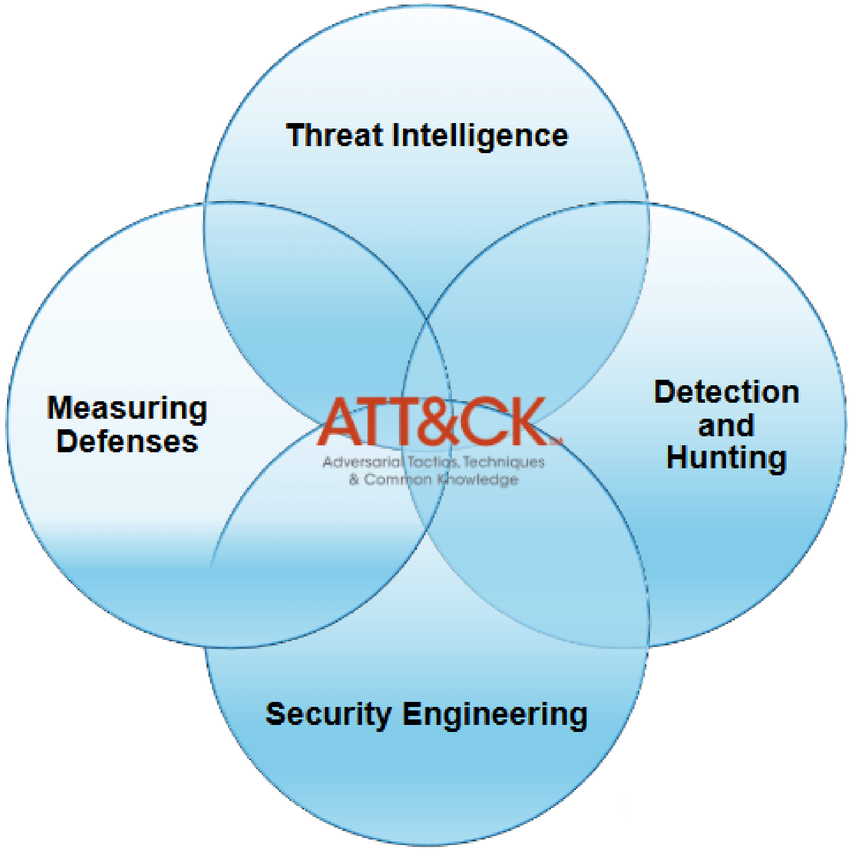


Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Image File Execution Options Injection			Forced Authentication	Network Share Discovery	AppleScript		Man in the Browser	Exfiltration Over Physical Medium	Multi-hop Proxy
Plist Modification			Hooking	System Time Discovery	Third-party Software		Browser Extensions		Domain Fronting
Valid Accounts			Password Filter DLL	Peripheral Device Discovery	Windows Remote Management		Video Capture	Exfiltration Over Command and Control Channel	Data Encoding
DLL Search Order Hijacking			LLMNR/NBT-NS Poisoning	Account Discovery	SSH Hijacking	LSASS Driver	Audio Capture		Remote File Copy
AppCert DLLs		Process Doppelgänging	Securityd Memory	File and Directory Discovery	Distributed Component Object Model	Dynamic Data Exchange	Automated Collection	Scheduled Transfer	Multi-Stage Channels
Hooking		Mshta	Private Keys	System Information Discovery		Mshta	Clipboard Data	Data Encrypted	Web Service
Startup Items		Hidden Files and Directories	Keychain		Pass the Ticket	Local Job Scheduling	Email Collection	Automated Exfiltration	Standard Non-Application Layer Protocol
Launch Daemon		Launchctl	Input Prompt	Security Software Discovery	Replication Through Removable Media	Trap	Screen Capture	Exfiltration Over Other Network Medium	
Dylib Hijacking		Space after Filename	Bash History			Source	Data Staged		Communication Through Removable Media
Application Shimming		LC_MAIN Hijacking	Two-Factor Authentication Interception	System Network Connections Discovery	Windows Admin Shares	Launchctl	Input Capture	Exfiltration Over Alternative Protocol	
AppInit DLLs		HISTCONTROL			Remote Desktop Protocol	Space after Filename	Data from Network Shared Drive		Multilayer Encryption
Web Shell		Hidden Users	Account Manipulation	System Owner/User Discovery	Pass the Hash	Execution through Module Load		Data Transfer Size Limits	Standard Application Layer Protocol
Service Registry Permissions Weakness		Clear Command History	Replication Through Removable Media		Exploitation of Vulnerability		Data from Local System	Data Compressed	
Scheduled Task		Gatekeeper Bypass		System Network Configuration Discovery	Shared Webroot	Regsvcs/Regasm	Data from Removable Media		Commonly Used Port
New Service		Hidden Window	Input Capture		Logon Scripts	InstallUtil			Standard Cryptographic Protocol
File System Permissions Weakness		Deobfuscate/Decode Files or Information	Network Sniffing	Application Window Discovery	Remote Services	Regsvr32			
Path Interception			Credential Dumping		Application Deployment Software	Execution through API			Custom Cryptographic Protocol
Accessibility Features		Trusted Developer Utilities	Brute Force	Network Service Scanning		PowerShell			
Port Monitors		Regsvcs/Regasm	Credentials in Files	Query Registry	Remote File Copy	Rundll32			Data Obfuscation
Screensaver	Exploitation of Vulnerability			Remote System Discovery	Taint Shared Content	Scripting			Custom Command and Control Protocol
LSASS Driver	Extra Window Memory Injection			Permission Groups Discovery		Graphical User Interface			
Browser Extensions	Access Token Manipulation					Command-Line Interface			Connection Proxy
Local Job Scheduling	Bypass User Account Control			Process Discovery		Scheduled Task			Uncommonly Used Port
Re-opened Applications	Process Injection			System Service Discovery		Windows Management Instrumentation			Multiband Communication
Rc.common	SID-History Injection	Component Object Model Hijacking							Fallback Channels
Login Item	Sudo					Trusted Developer Utilities			
LC_LOAD_DYLIB Addition	Setuid and Setgid	InstallUtil				Service Execution			
Launch Agent		Regsvr32							
Hidden Files and Directories		Code Signing							
.bash_profile and .bashrc		Modify Registry							
Trap		Component Firmware							
Launchctl		Redundant Access							
Office Application Startup		File Deletion							
Create Account		Timestomp							
External Remote Services		NTFS Extended Attributes							
Authentication Package		Process Hollowing							
Netsh Helper DLL		Disabling Security Tools							
Component Object Model Hijacking		Rundll32							
		DLL Side-Loading							
Redundant Access		Indicator Removal on Host							
Security Support Provider		Indicator Removal from Tools							
Windows Management Instrumentation Event Subscription									
		Indicator Blocking							
		Software Packing							
Registry Run Keys / Start Folder		Masquerading							
		Obfuscated Files or Information							
Change Default File Association									
		Binary Padding							
Component Firmware		Install Root Certificate							
Bootkit		Network Share Connection Removal							
Hypervisor									
Logon Scripts		Rootkit							
Modify Existing Service		Scripting							

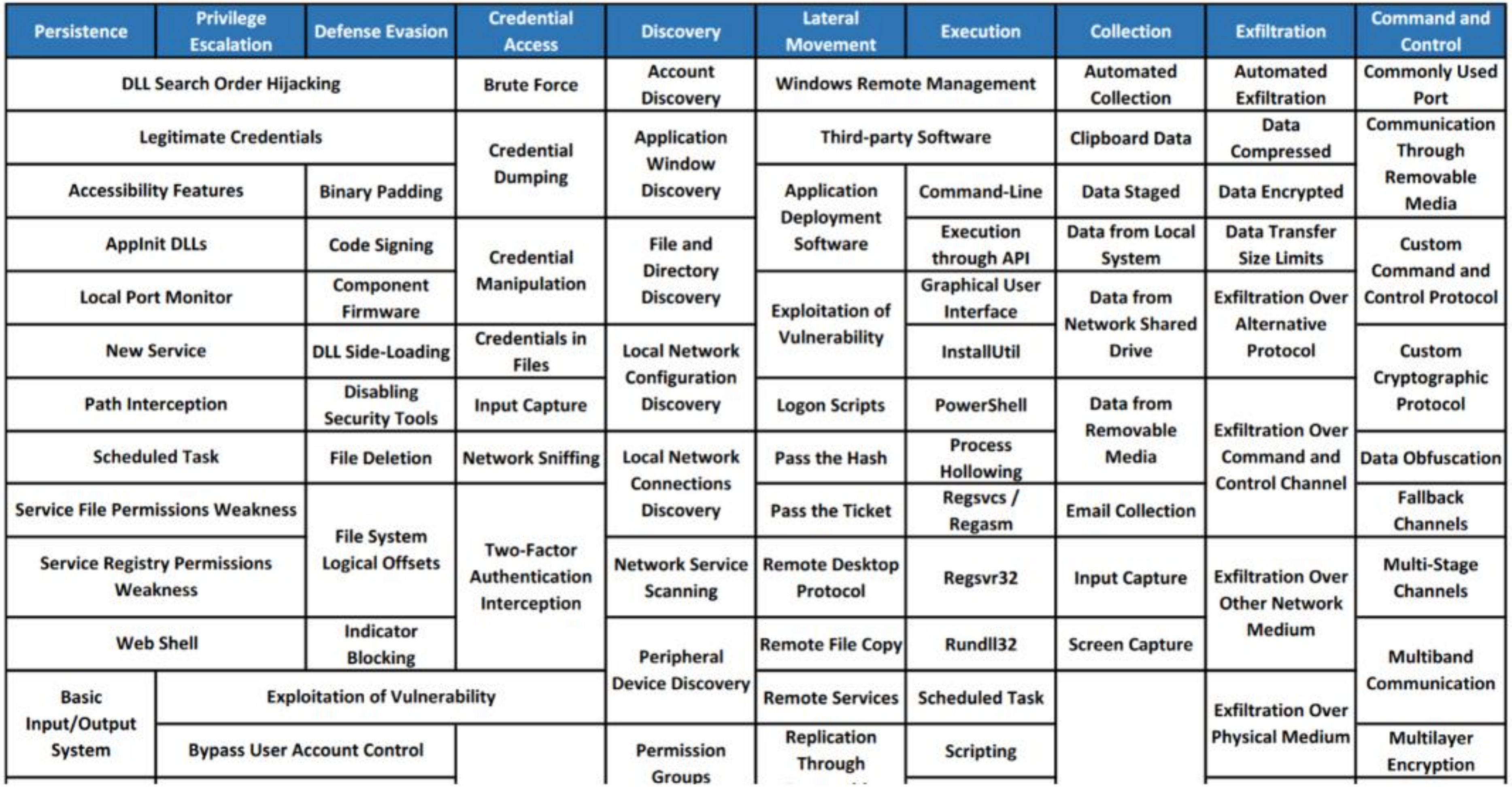
attack.mitre.org

The ATT&CK Use Case

- **Improve security posture through gap analysis, prioritization, and remediation**
  - Use ATT&CK to guide threat hunting campaigns
  - Emulate adversaries to measure defenses against relevant threats
  - Leverage *threat intelligence* to prioritize technique detection
  - Remediate gaps by mapping solutions back to the ATT&CK threat model



MITRE ATT&CK Matrix

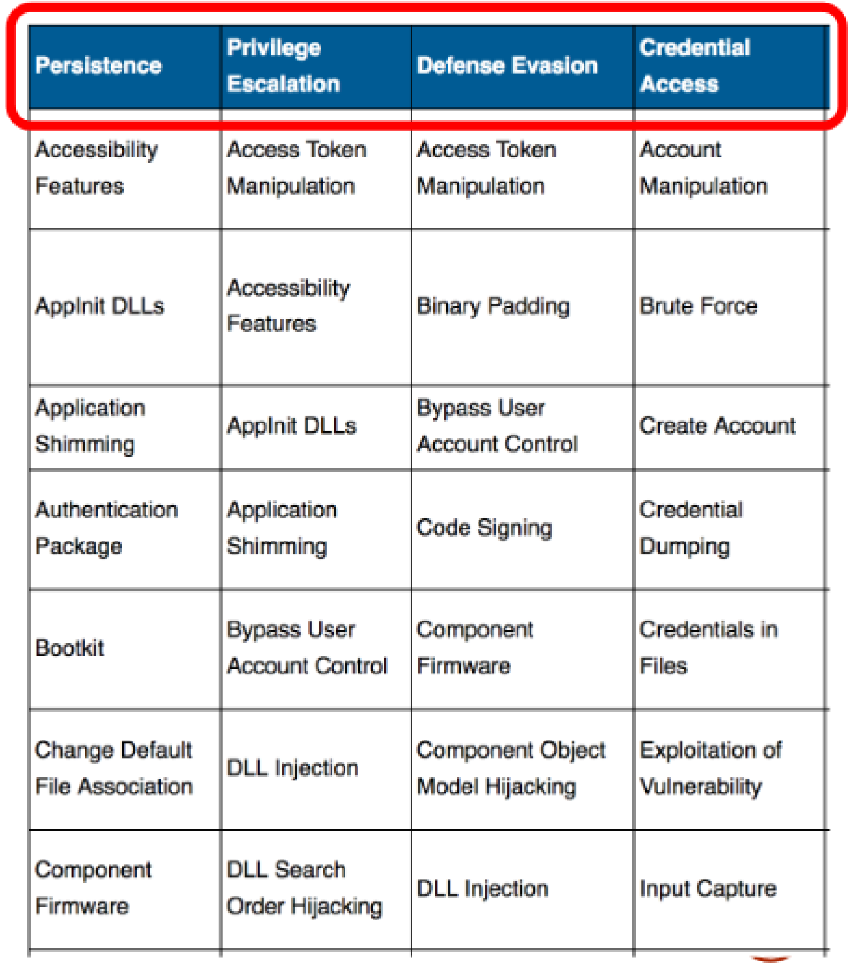


Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
DLL Search Order Hijacking			Brute Force	Account Discovery	Windows Remote Management		Automated Collection	Automated Exfiltration	Commonly Used Port
Legitimate Credentials			Credential Dumping	Application Window Discovery	Third-party Software		Clipboard Data	Data Compressed	Communication Through Removable Media
Accessibility Features		Binary Padding			Application Deployment Software	Command-Line	Data Staged	Data Encrypted	
AppInit DLLs		Code Signing	Credential Manipulation	File and Directory Discovery		Execution through API	Data from Local System	Data Transfer Size Limits	Custom Command and Control Protocol
Local Port Monitor		Component Firmware			Exploitation of Vulnerability	Graphical User Interface	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	
New Service		DLL Side-Loading	Credentials in Files	Local Network Configuration Discovery		InstallUtil			Custom Cryptographic Protocol
Path Interception		Disabling Security Tools	Input Capture		Logon Scripts	PowerShell	Data from Removable Media	Exfiltration Over Command and Control Channel	
Scheduled Task		File Deletion	Network Sniffing	Local Network Connections Discovery	Pass the Hash	Process Hollowing			Data Obfuscation
Service File Permissions Weakness		File System Logical Offsets	Two-Factor Authentication Interception		Pass the Ticket	Regsvcs / Regasm	Email Collection		Fallback Channels
Service Registry Permissions Weakness				Network Service Scanning	Remote Desktop Protocol	Regsvr32	Input Capture	Exfiltration Over Other Network Medium	Multi-Stage Channels
Web Shell		Indicator Blocking		Peripheral Device Discovery	Remote File Copy	Rundll32	Screen Capture		Multiband Communication
Basic Input/Output System	Exploitation of Vulnerability				Remote Services	Scheduled Task		Exfiltration Over Physical Medium	
	Bypass User Account Control			Permission Groups	Replication Through	Scripting			Multilayer Encryption

MITRE ATT&CK Matrix

HOW DO I READ IT?

- **Tactics** across the top
    - What the techniques accomplish

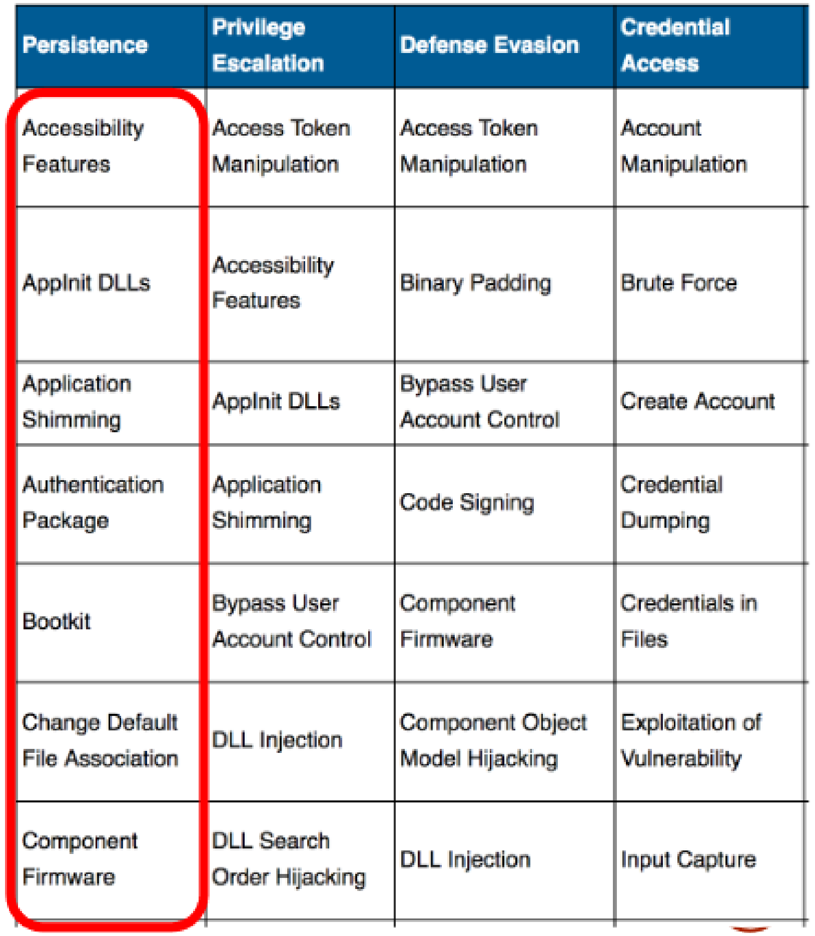


Persistence	Privilege Escalation	Defense Evasion	Credential Access
Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation
AppInit DLLs	Accessibility Features	Binary Padding	Brute Force
Application Shimming	AppInit DLLs	Bypass User Account Control	Create Account
Authentication Package	Application Shimming	Code Signing	Credential Dumping
Bootkit	Bypass User Account Control	Component Firmware	Credentials in Files
Change Default File Association	DLL Injection	Component Object Model Hijacking	Exploitation of Vulnerability
Component Firmware	DLL Search Order Hijacking	DLL Injection	Input Capture

MITRE ATT&CK Matrix

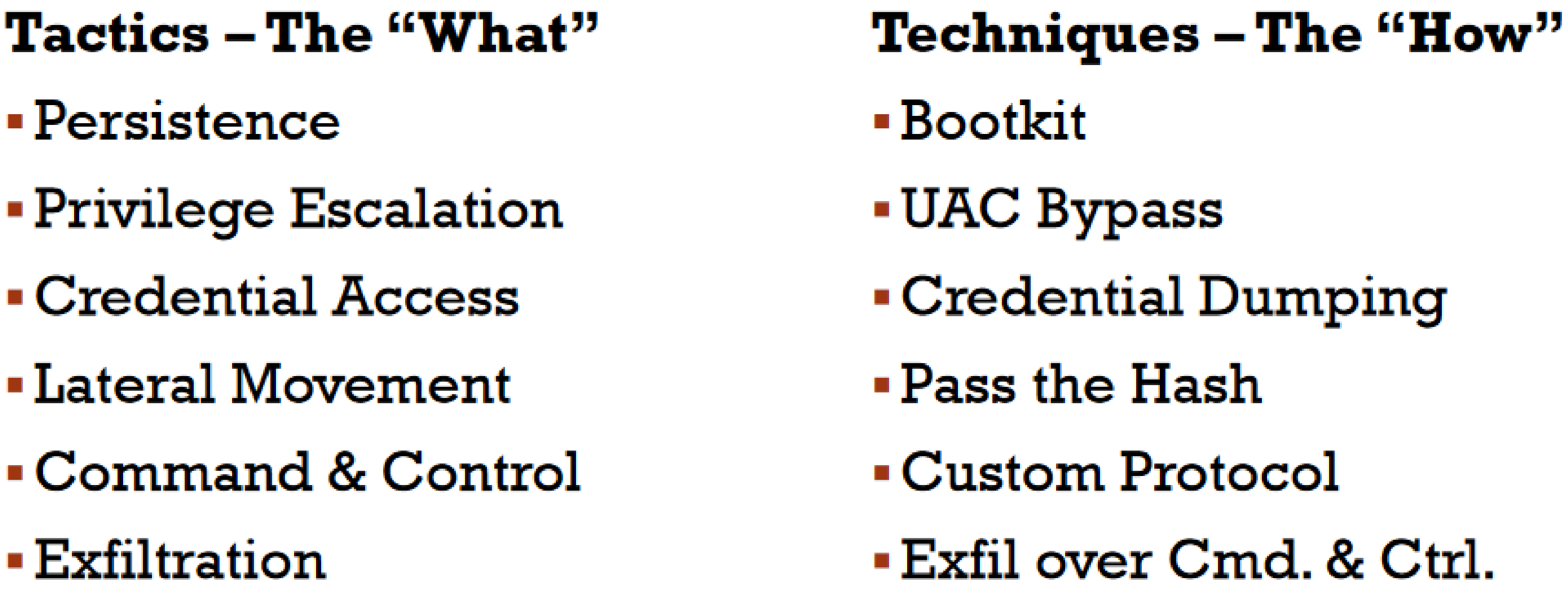
HOW DO I READ IT?

- **Tactics** across the top
  - What the techniques accomplish
- **Techniques** in each column
  - All known ways of accomplishing that tactic



Persistence	Privilege Escalation	Defense Evasion	Credential Access
Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation
AppInit DLLs	Accessibility Features	Binary Padding	Brute Force
Application Shimming	AppInit DLLs	Bypass User Account Control	Create Account
Authentication Package	Application Shimming	Code Signing	Credential Dumping
Bootkit	Bypass User Account Control	Component Firmware	Credentials in Files
Change Default File Association	DLL Injection	Component Object Model Hijacking	Exploitation of Vulnerability
Component Firmware	DLL Search Order Hijacking	DLL Injection	Input Capture

Tactic Vs Technique



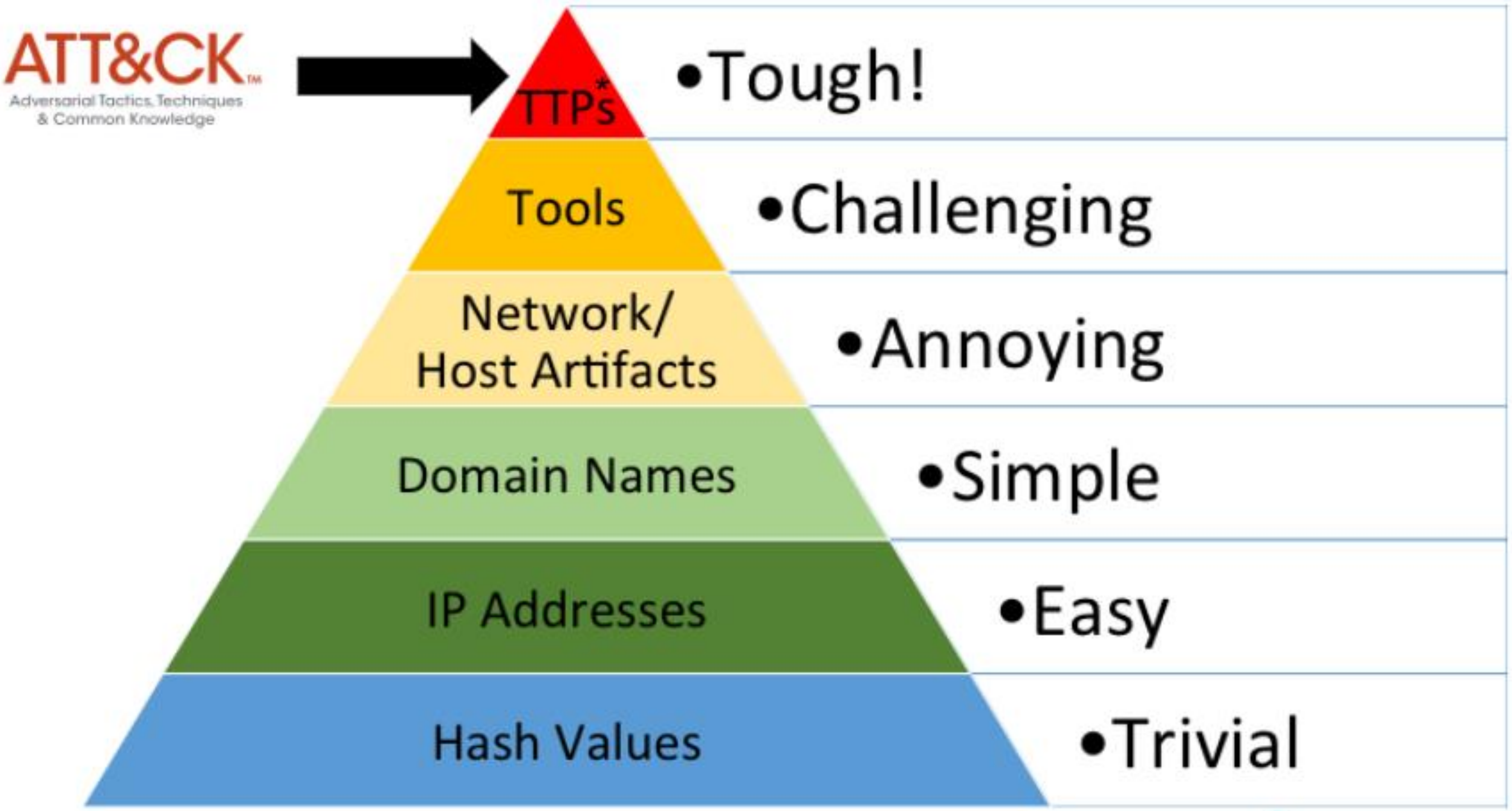
Tactics – The “What”

- Persistence
- Privilege Escalation
- Credential Access
- Lateral Movement
- Command & Control
- Exfiltration

Techniques – The “How”

- Bootkit
- UAC Bypass
- Credential Dumping
- Pass the Hash
- Custom Protocol
- Exfil over Cmd. & Ctrl.

Pyramid of Pain

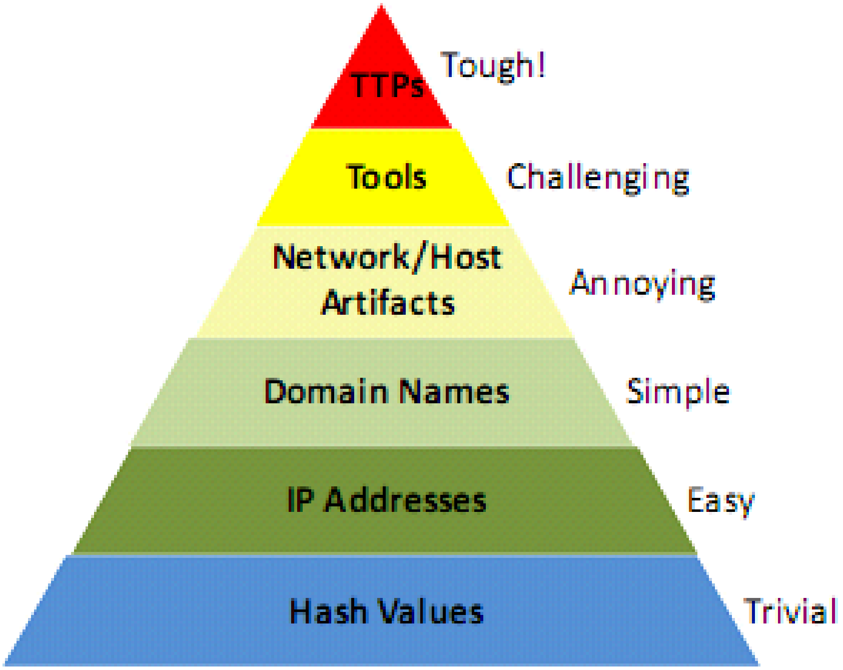


Pyramid of Pain

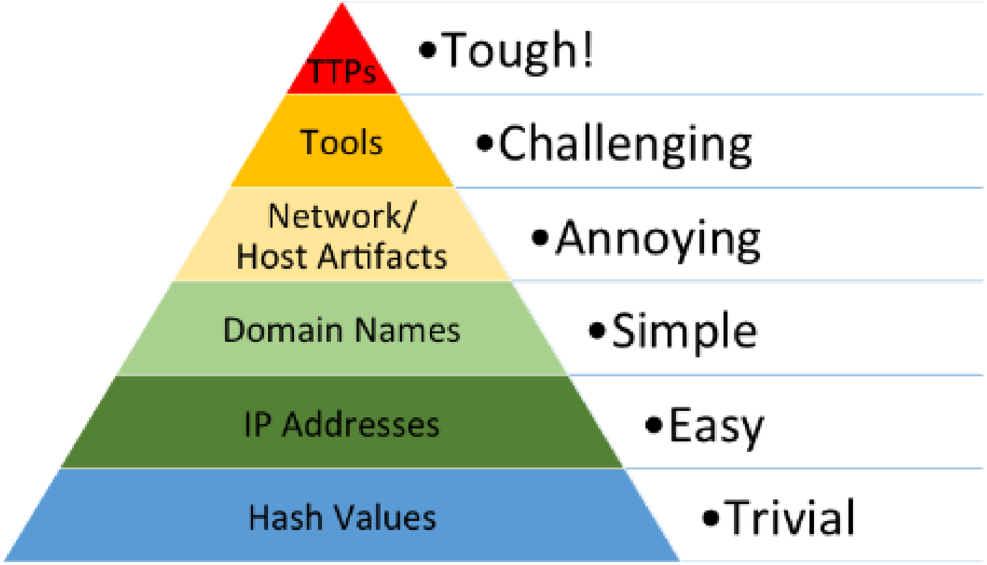
- Pyramid of Pain represents the types of indicators that the analyst must look out to **detect the activities of an adversary** as well as the amount of pain that the adversary needs to adapt to pivot and continue with the attack even when the indicators at each level are being denied.

- It consists of **six types of IoCs** that are arranged in increasing order of the impact on the adversary and effort of the analyst, respectively.

- **IoC on the bottom** of the pyramid will **have less impact** on the adversary, whereas **IoC placed on the top** would not only have a **huge impact** but would also require vast amount of effort by the analyst for its disclosure.



Pyramid of Pain



TTPs	•Tough!
Tools	•Challenging
Network/ Host Artifacts	•Annoying
Domain Names	•Simple
IP Addresses	•Easy
Hash Values	•Trivial

The Pyramid measures **potential usefulness** of your intel

It also measures **difficulty of obtaining** that intel

The higher you are, the **more resources** your adversaries have to expend.

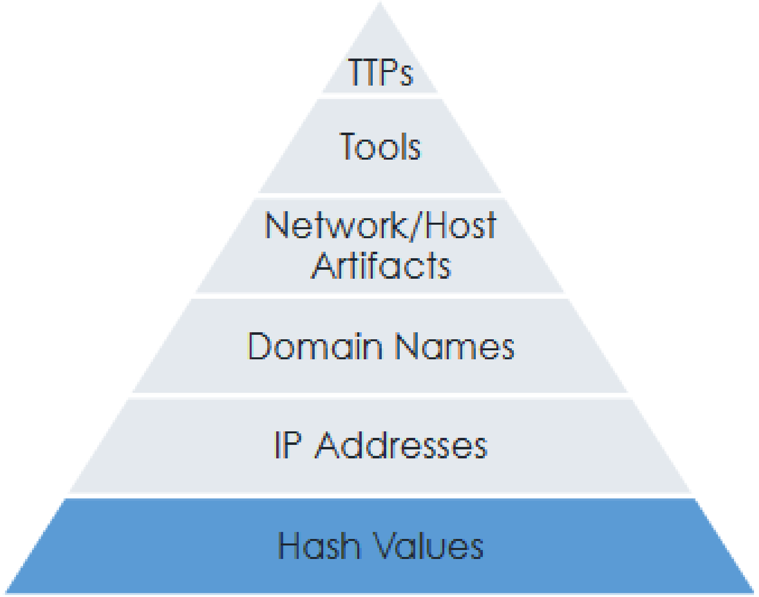
When you quickly detect, respond to and disrupt your adversaries' activities, defense becomes offense.

Pyramid of Pain : Hashes

Hashes are, by far, the highest confidence indicators.

Unfortunately, they are extremely susceptible to change (even accidentally).

Hashes are probably the least useful type of indicators.



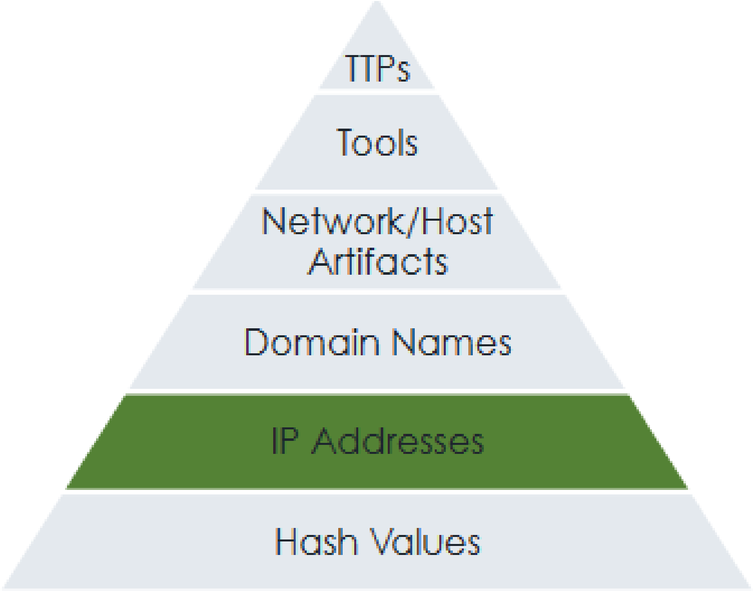
MD5
5f6ce162c4b5516670d5a8f1f8f4e57b
SHA1
C8d4c389beaff88811f8fab1965519fce74ffd8a
SHA256
ad690662a1faf97dc41387b73f8fd3415d64f9b0ce66db3e9134385d94e0c01b

Pyramid of Pain : IP Address

Only n00bs use their own addresses.

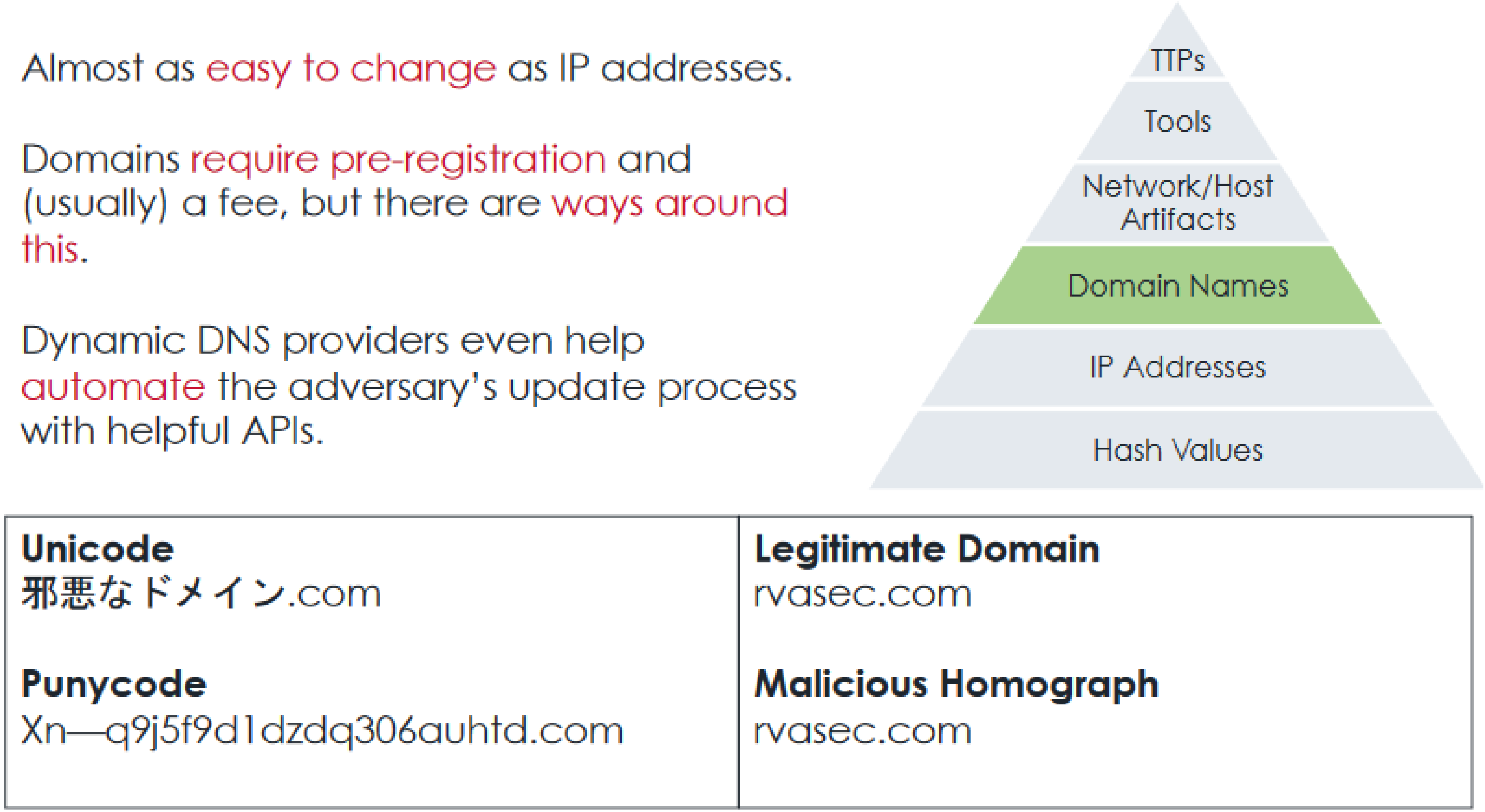
VPNs, Tor, open proxies all make it trivial to change your IP.

If it's hardcoded into a config, maybe adversaries have to do a little work to update it.



Dotted Decimal 192.168.1.1	**Decimal** 3232235777
Dotted Hex 0xC0.0xA8.0x01.0x01	**Hex** 0xC0A80101
Dotted Octal 0300.0250.0001.0001	**Octal** 030052000401

Pyramid of Pain : Domain



Almost as easy to change as IP addresses.

Domains require pre-registration and (usually) a fee, but there are ways around this.

Dynamic DNS providers even help automate the adversary's update process with helpful APIs.

TTPs

Tools

Network/Host Artifacts

Domain Names

IP Addresses

Hash Values

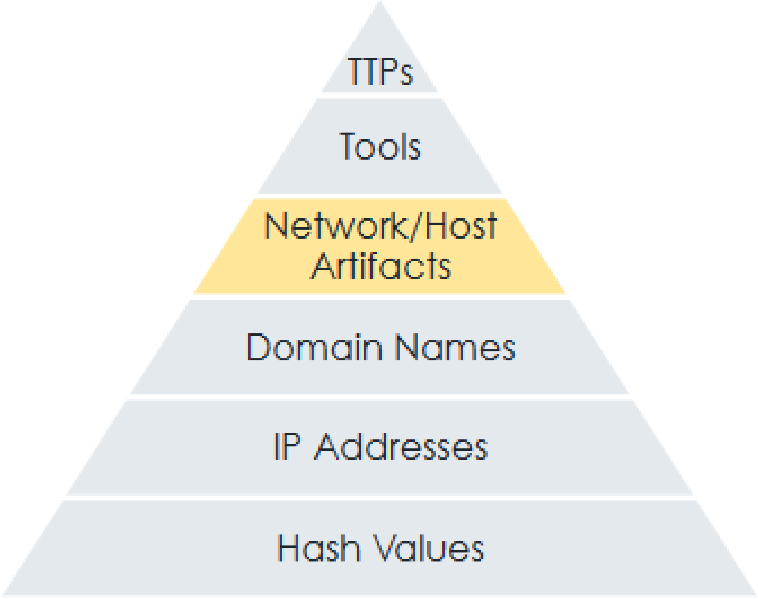
Unicode 邪悪なドメイン.com **Punycode** Xn—q9j5f9d1dzdq306auhtd.com	**Legitimate Domain** rvasec.com **Malicious Homograph** rvasec.com

Pyramid of Pain : Network / Host Artifact

It's very difficult to perform useful activities without leaving some traces.

On hosts, look for files & directories, registry objects, mutexes, memory strings […]

On the network, check for distinctive transaction values, especially protocol errors or just misinterpretations.



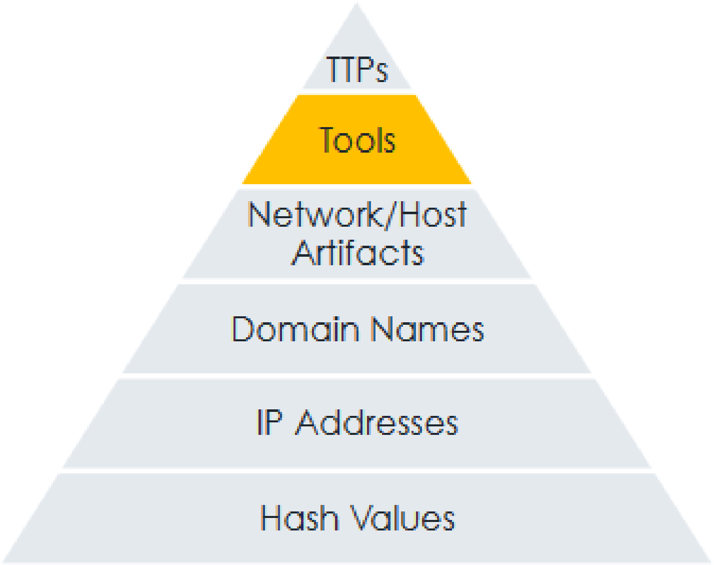
Distinctive URI patterns
/^[A-F0-9]{16}\/\d{3,5}\.{php|aspx}$/
User-Agent Strings
xi/1.0
Typos
Mozilla/5.0 (compatible; MSIE7.0; Windows NT 6.1;)

Pyramid of Pain : Tools

If you see the same tool over and over, you eventually get really good at detecting it.

No matter what incidental changes they make, your detection mechanisms can deal with them.

To continue, they need a new tool. With testing & training time, that's a real victory!



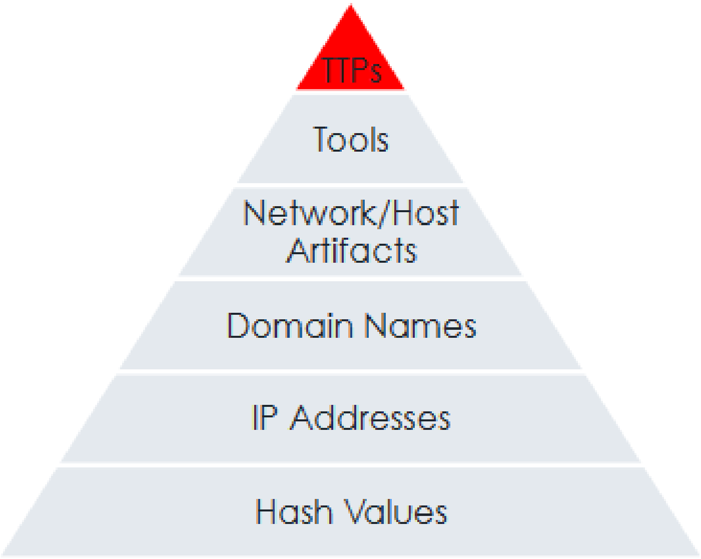
Once upon a time, there was an incident response team who encountered the same tool over and over again for more than a year. The tool had a bolt-on network front end, so the attackers could easily change the network protocol, but the back end was always the same. Eventually, the IR team realized that the distinctive keep-alive function was part of the back end, and could be reliably detected. And then everyone (except the attacker) slept well at night and lived happily ever after!

Pyramid of Pain : TTPs

TTPs are the expression of the attacker's training.

Retraining is probably the hardest thing you can do once, let alone continually.

This becomes so expensive that they have to question their commitment to attacking you. Win!



Data Staging Tactic
Create encrypted RAR and transfer them to the exfiltration point.
Data Staging Technique
AES encryption, files of exactly 650,000 bytes, file copies via SMB
Data Staging Procedure
winrar a –hpqwerty –r vacation_photos.rar *staging_dir*
net use \exfil_server\photos

Why Should Blue Team Love MITRE ATT&CK

- Assessment and Engineering
- Measuring Detection Coverage and Critical Security Control Based on MITRE ATT&CK
- Aligning Actionable Threat Intelligence into MITRE ATT&CK
- Perform Red Team and Blue Team Adversary Simulation Based on MITRE ATT&CK
- Using MITRE ATT&CK to Mature Threat Hunting Program

Why Should Blue Team Love MITRE ATT&CK

Assessment and Engineering

- **Drive decisions about what you collect (and buy) based on visibility**
  - Where are your gaps?
  - What other tools can you choose?
  - Will they help you build more effective defenses?
- **Help you move toward a broader view of security beyond just detection**
- **Increase awareness of where you may need to accept risk**
  - What *can't* you detect or mitigate?

Why Should Blue Team Love MITRE ATT&CK

Assessment and Engineering (Cont’d..)

- **Collect *one* log source that will improve your ATT&CK visibility**
  - Especially if you’re struggling to write many detections
- **Places to start (that cost nothing but time):**
  - Windows Event Logs
    - Malware Archaeology Cheat Sheets (including ATT&CK): https://www.malwarearchaeology.com/cheat-sheets/
    - NCSC Logging Made Easy: https://github.com/ukncsc/lme/
  - Sysmon
    - SwiftonSecurity sysmon-config: https://github.com/SwiftOnSecurity/sysmon-config

Why Should Blue Team Love MITRE ATT&CK

Assessment and Engineering (Cont’d..)

- **Assess your ATT&CK coverage map *beyond* just detection**
- **What can you mitigate?**
  - Can you mitigate with tools?
  - Can you mitigate with policies? (People and process matter too!)
- **What *can’t* you detect or mitigate?**
  - May need to accept risk

Why Should Blue Team Love MITRE ATT&CK

Assessment and Engineering (Cont'd..)

- **Plan out your tool and log acquisition strategy based on coverage**
- **Determine what techniques your current logs and tools detect and mitigate**
  - Review documentation for the tool
  - Ask the vendor
  - Validate tool output
- **Consider what changes you could make to your environment**
  - Should you change configurations of an existing tool?
  - Should you acquire a new tool?
  - What gaps would that tool help you fill?
- **Examine your security budget and plan for the best use of resources**

Why Should Blue Team Love MITRE ATT&CK

Measuring Detection Coverage and Critical Security Control Based on MITRE ATT&CK

- Defensive controls can carry well-understood meaning when referenced against the ATT&CK tactics and techniques they apply to.
- Assess your detection coverage across ATT&CK
- Improve focus on post-exploit activity (in addition to perimeter defenses)
- Move toward detecting adversary TTPs in addition to indicators
- Organize detections to enable:
  - Finding gaps in coverage
  - Tracking improvement over time
- Look at others' behavioral analytics and choose a few to implement
- Adapt them to your environment (tuning needed!)

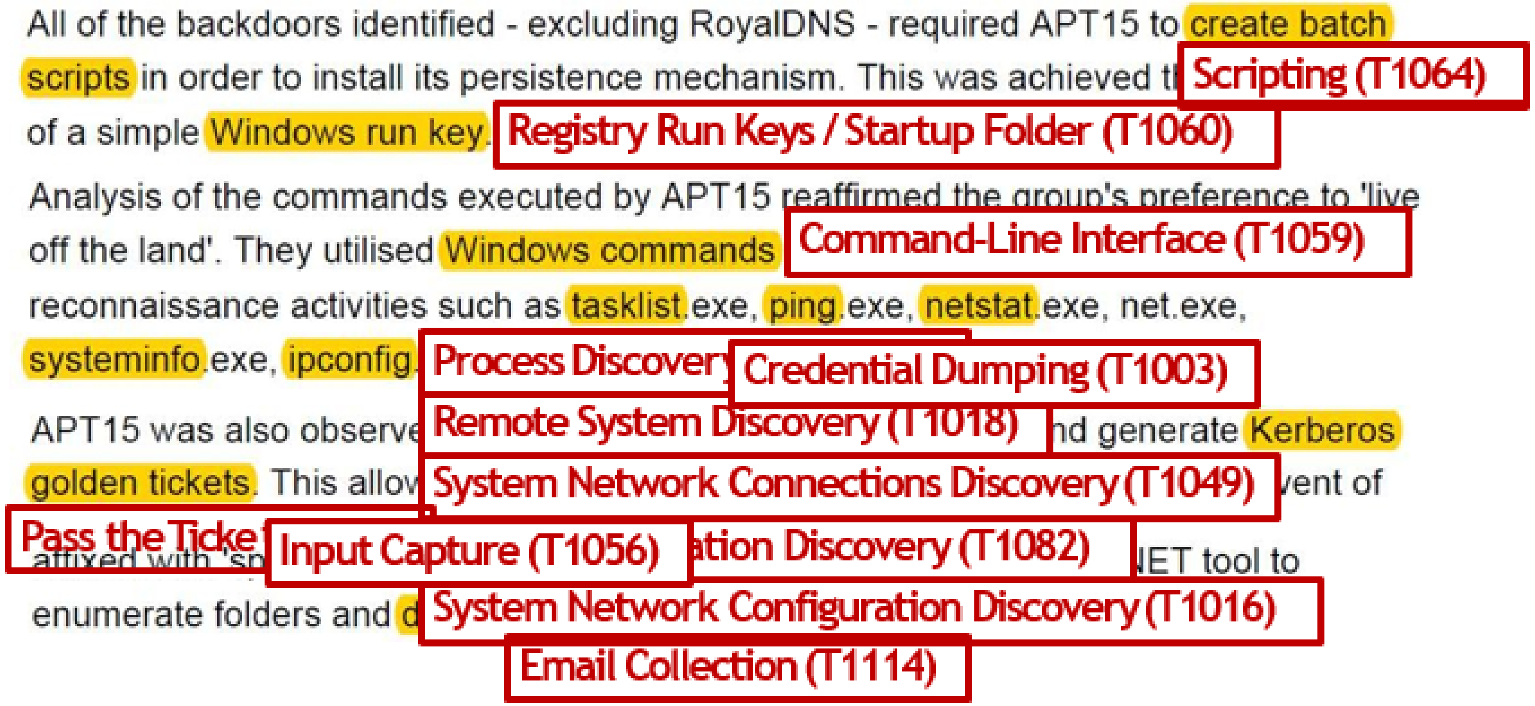
Why Should Blue Team Love MITRE ATT&CK

Aligning Actionable Threat Intelligence into MITRE ATT&CK

- **Use knowledge of adversary behaviors to help inform defenders**
- **Structuring threat intelligence with ATT&CK allows us to…**
  - *Compare* behaviors
    - Groups to each other
    - Groups over time
    - Groups to defenses
  - *Communicate* in a common language
    - Across teams in your organization
    - Across organizations
- **Make recommendations to your defenders on how to detect and mitigate the group's techniques**

Why Should Blue Team Love MITRE ATT&CK

Aligning Actionable Threat Intelligence into MITRE ATT&CK (Cont'd…)



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

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 … nd generate Kerberos golden tickets. This allow … vent of

affixed with 'sp … NET tool to

enumerate folders and d

Scripting (T1064)

Registry Run Keys / Startup Folder (T1060)

Command-Line Interface (T1059)

Process Discovery

Credential Dumping (T1003)

Remote System Discovery (T1018)

System Network Connections Discovery (T1049)

Pass the Ticke

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/

Why Should Blue Team Love MITRE ATT&CK

Perform Red Team and Blue Team Adversary Simulation Based on MITRE ATT&CK

- **You think you know what you can detect and mitigate…**
  - …but how can you be sure? Are there adversaries in your network?

    -> Enter red teamers!
- **Use ATT&CK to organize your red team plans**
- **Move toward adversary emulation**
  - Subset of threat-based security testing
  - Emulate the techniques of real adversaries
  - Focus on the technique behaviors

Why Should Blue Team Love MITRE ATT&CK

Perform Red Team and Blue Team Adversary Simulation Based on MITRE ATT&CK (Cont'd..)

- **No red team? No problem!**
- **Defenders can try out red teaming tools to get your feet wet**
  - CALDERA: https://github.com/mitre/caldera
  - Red Team Automation: https://github.com/endgameinc/RTA
  - Metta: https://github.com/uber-common/metta

Perform Red Team and Blue Team Adversary Simulation Based on MITRE ATT&CK (Cont'd..)

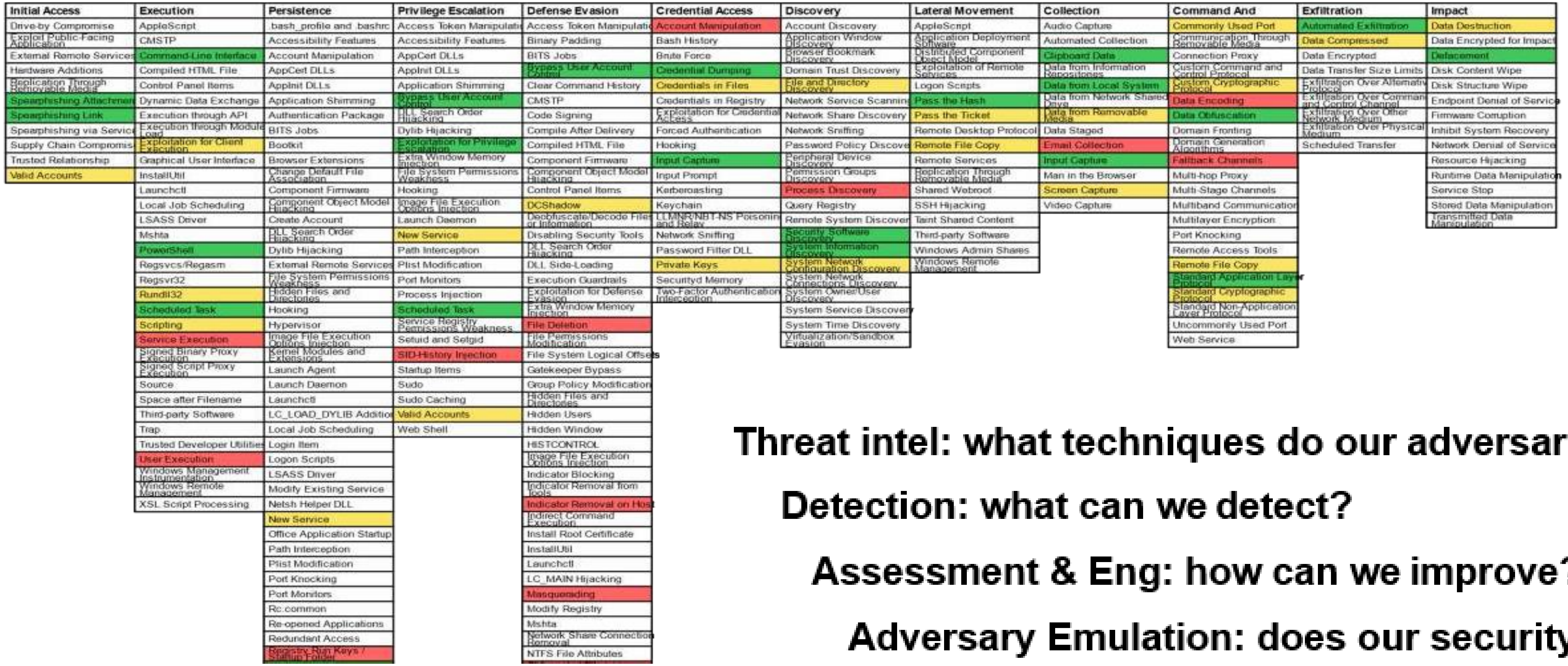
- **Use ATT&CK to mature what your red team is doing**
  - Have your team choose a different ATT&CK technique each week
  - Discuss how you'd use different procedures to perform the behavior
  - Bring in your threat intel analysts to talk about how adversaries are using it
  - Communicate with your blue team in a common language
- **Have your red team start emulating ATT&CK techniques themselves**
  - APT3 Adversary Emulation Plan: https://attack.mitre.org/resources/adversary-emulation-plans/

Why Should Blue Team Love MITRE ATT&CK

Using MITRE ATT&CK to Mature Threat Hunting Program

- One of the best uses of the ATT&CK framework is to use it to understand how durable your defenses are for each attack behavior. Phil Hagen, Senior SANS Instructor, states that testing against the ATT&CK framework "provides you a shopping list of where you need to focus your attention and resources."
- If your Security Operations Center (SOC) already uses a kill chain model, the ATT&CK framework aligns well and can be used in coordination with it. ATT&CK looks at the ways that an attacker would execute on a cyber kill chain. **The ATT&CK framework makes it more granular and allows threat hunters to test and act on this information**.
- Really, it's all about testing your defenses. The ATT&CK framework just gives you a way to categorize your results so you can identify where to focus for optimizing your cybersecurity.

Bringing All Together



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulati	Access Token Manipulatio	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternativ Protocol	Disk Structure Wipe
Spearphishing Attachmen	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scannin	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Comman and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Servic	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromis	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discove	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Resource Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy		Runtime Data Manipulation
	Launchctl	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels		Service Stop
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	SSH Hijacking	Video Capture	Multiband Communication		Stored Data Manipulation
	LSASS Driver	Create Account	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisonin and Relay	Remote System Discover	Taint Shared Content		Multilayer Encryption		Transmitted Data Manipulation
	Mshta	DLL Search Order Hijacking	New Service	Disabling Security Tools	Network Sniffing	Security Software Discovery	Third-party Software		Port Knocking		
	PowerShell	Dylib Hijacking	Path Interception	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools		
	Regsvcs/Regasm	External Remote Services	Plist Modification	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Remote File Copy		
	Regsvr32	File System Permissions Weakness	Port Monitors	Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard Application Layer Protocol		
	Rundll32	Hidden Files and Directories	Process Injection	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Owner/User Discovery			Standard Cryptographic Protocol		
	Scheduled Task	Hooking	Scheduled Task	Extra Window Memory Injection		System Service Discovery			Standard Non-Application Layer Protocol		
	Scripting	Hypervisor	Service Registry Permissions Weakness	File Deletion		System Time Discovery			Uncommonly Used Port		
	Service Execution	Image File Execution Options Injection	Setuid and Setgid	File Permissions Modification		Virtualization/Sandbox Evasion			Web Service		
	Signed Binary Proxy Execution	Kernel Modules and Extensions	SID-History Injection	File System Logical Offsets							
	Signed Script Proxy Execution	Launch Agent	Startup Items	Gatekeeper Bypass							
	Source	Launch Daemon	Sudo	Group Policy Modification							
	Space after Filename	Launchctl	Sudo Caching	Hidden Files and Directories							
	Third-party Software	LC_LOAD_DYLIB Additio	Valid Accounts	Hidden Users							
	Trap	Local Job Scheduling	Web Shell	Hidden Window							
	Trusted Developer Utilities	Login Item		HISTCONTROL							
	User Execution	Logon Scripts		Image File Execution Options Injection							
	Windows Management Instrumentation	LSASS Driver		Indicator Blocking							
	Windows Remote Management	Modify Existing Service		Indicator Removal from Tools							
	XSL Script Processing	Netsh Helper DLL		Indicator Removal on Host							
		New Service		Indirect Command Execution							
		Office Application Startup		Install Root Certificate							
		Path Interception		InstallUtil							
		Plist Modification		Launchctl							
		Port Knocking		LC_MAIN Hijacking							
		Port Monitors		Masquerading							
		Rc.common		Modify Registry							
		Re-opened Applications		Mshta							
		Redundant Access		Network Share Connection Removal							
		Registry Run Keys / Startup Folder		NTFS File Attributes							

Threat intel: what techniques do our adversaries use?

Detection: what can we detect?

Assessment & Eng: how can we improve?

Adversary Emulation: does our security hold up?

SUMMARY AND KEY TAKEAWAYS

- **ATT&CK can help you create a threat-informed defense**
- **Do what you can, with what you have, where you are:**
  - Detection
  - Assessment and Engineering
  - Threat Intelligence
  - Adversary Emulation
  - Threat Hunting
- **Choose a starting point that works for your team**