MITRE ATT&CK™ Update

Richard Struse

Chief Strategist for Cyber Threat Intelligence

What is ATT&CK?

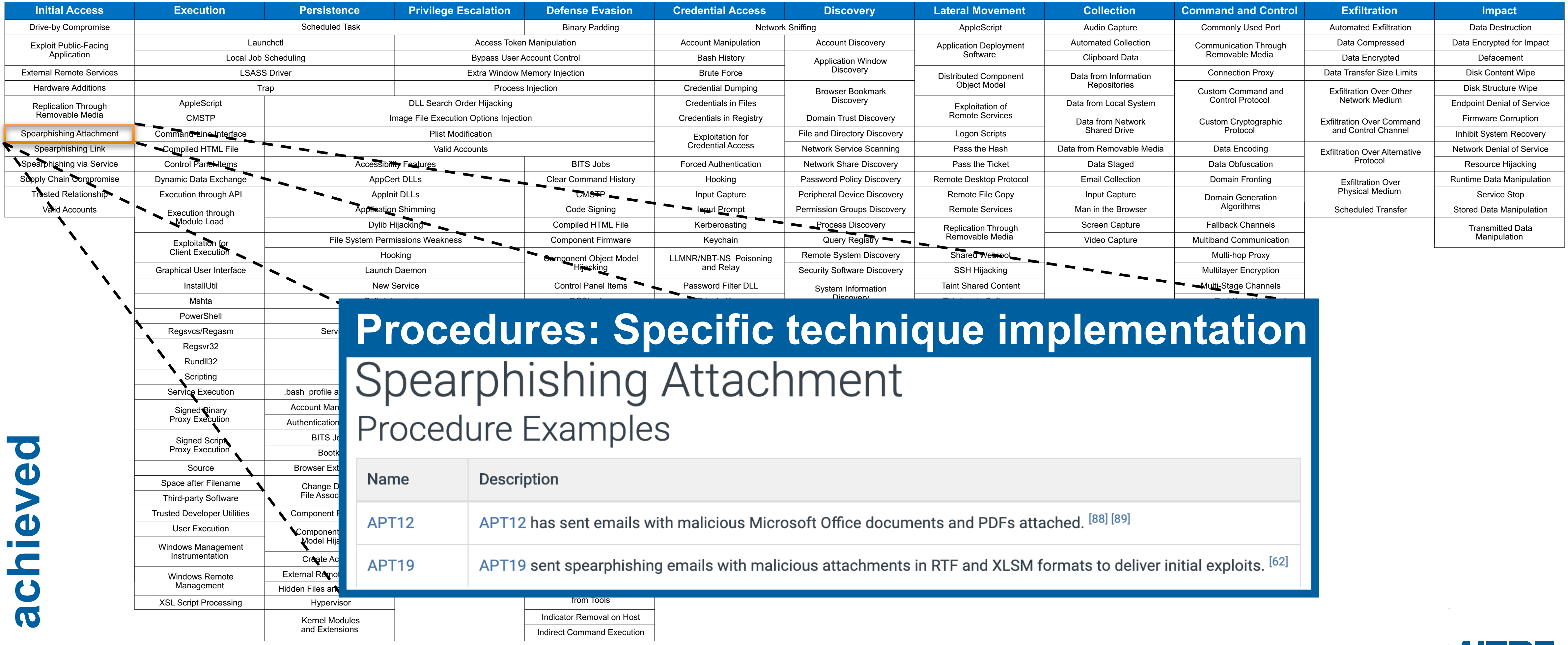
A knowledge base of adversary behavior

- *Based on real-world observations*
- *Free, open, and globally accessible*
- *A common language*
- *Community-driven*

ATT&CK Today

Techniques: how the goals are achieved

Tactics: the adversary’s technical goals



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										
	Regsvcs/Regasm	Serv									
	Regsvr32										
	Rundll32										
	Scripting										
	Service Execution	.bash_profile a									
	Signed Binary Proxy Execution	Account Man									
		Authentication									
	Signed Script Proxy Execution	BITS Jo									
		Bootk									
	Source	Browser Ext									
	Space after Filename	Change D File Assoc									
	Third-party Software										
	Trusted Developer Utilities	Component F									
	User Execution	Component Model Hija									
	Windows Management Instrumentation										
		Create Ac									
	Windows Remote Management	External Remot									
		Hidden Files an									
	XSL Script Processing	Hypervisor		from Tools							
		Kernel Modules and Extensions		Indicator Removal on Host							
				Indirect Command Execution							

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]

What's Next for ATT&CK: "One ATT&CK"

- **Consistency and integration between matrices**
  - Refactor PRE-ATT&CK as part of this

Mobile ATT&CK

Enterprise ATT&CK

PRE-ATT&CK

It's just

ATT&CK™

MITRE

October 2019 Update

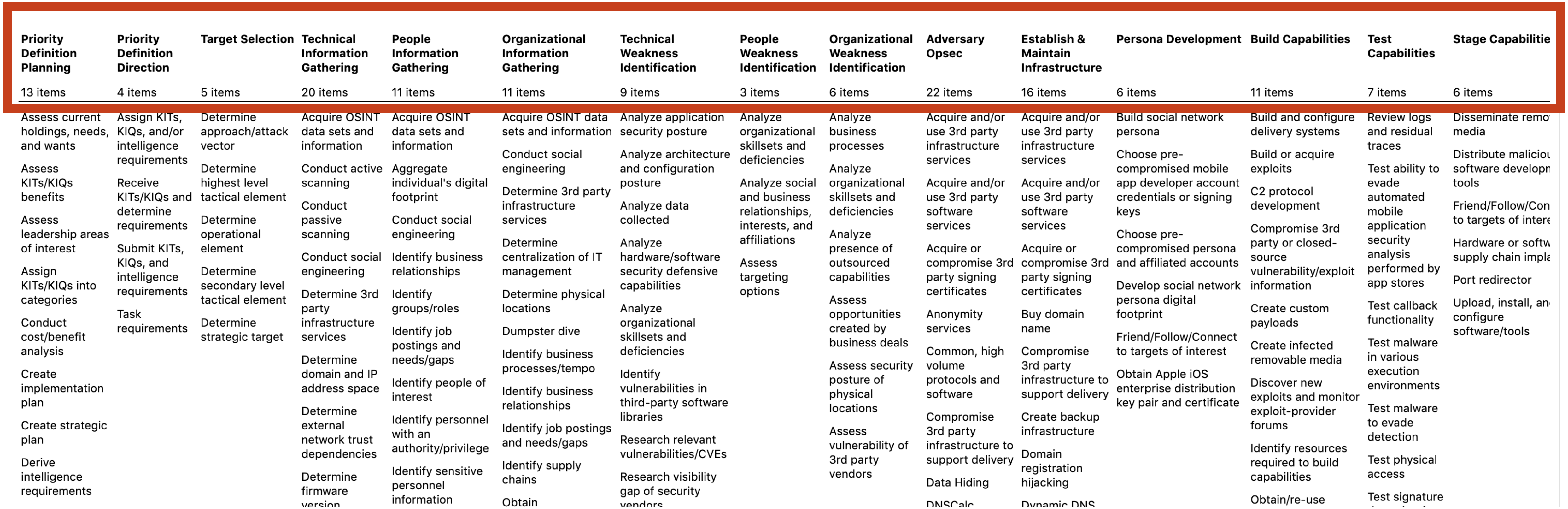
Release notes available at:

https://attack.mitre.org/resources/updates/

PRE-ATT&CK

Pre-ATT&CK Today

15 Tactics & ~144 Techniques



Priority Definition Planning	Priority Definition Direction	Target Selection	Technical Information Gathering	People Information Gathering	Organizational Information Gathering	Technical Weakness Identification	People Weakness Identification	Organizational Weakness Identification	Adversary Opsec	Establish & Maintain Infrastructure	Persona Development	Build Capabilities	Test Capabilities	Stage Capabilitie
13 items	4 items	5 items	20 items	11 items	11 items	9 items	3 items	6 items	22 items	16 items	6 items	11 items	7 items	6 items
Assess current holdings, needs, and wants	Assign KITs, KIQs, and/or intelligence requirements	Determine approach/attack vector	Acquire OSINT data sets and information	Acquire OSINT data sets and information	Acquire OSINT data sets and information	Analyze application security posture	Analyze organizational skillsets and deficiencies	Analyze business processes	Acquire and/or use 3rd party infrastructure services	Acquire and/or use 3rd party infrastructure services	Build social network persona	Build and configure delivery systems	Review logs and residual traces	Disseminate remo media
Assess KITs/KIQs benefits	Receive KITs/KIQs and determine requirements	Determine highest level tactical element	Conduct active scanning	Aggregate individual's digital footprint	Conduct social engineering	Analyze architecture and configuration posture	Analyze social and business relationships, interests, and affiliations	Analyze organizational skillsets and deficiencies	Acquire and/or use 3rd party software services	Acquire and/or use 3rd party software services	Choose pre-compromised mobile app developer account credentials or signing keys	Build or acquire exploits	Test ability to evade automated mobile application security analysis performed by app stores	Distribute maliciou software developn tools
Assess leadership areas of interest	Submit KITs, KIQs, and intelligence requirements	Determine operational element	Conduct passive scanning	Conduct social engineering	Determine 3rd party infrastructure services	Analyze data collected	Assess targeting options	Analyze presence of outsourced capabilities	Acquire or compromise 3rd party signing certificates	Acquire or compromise 3rd party signing certificates	Choose pre-compromised persona and affiliated accounts	C2 protocol development	Test callback functionality	Friend/Follow/Con to targets of intere
Assign KITs/KIQs into categories	Task requirements	Determine secondary level tactical element	Conduct social engineering	Identify business relationships	Determine centralization of IT management	Analyze hardware/software security defensive capabilities		Assess opportunities created by business deals	Anonymity services	Buy domain name	Develop social network persona digital footprint	Compromise 3rd party or closed-source vulnerability/exploit information	Test malware in various execution environments	Hardware or softw supply chain impla
Conduct cost/benefit analysis		Determine strategic target	Determine 3rd party infrastructure services	Identify groups/roles	Determine physical locations	Analyze organizational skillsets and deficiencies		Assess security posture of physical locations	Common, high volume protocols and software	Compromise 3rd party infrastructure to support delivery	Friend/Follow/Connect to targets of interest	Create custom payloads	Test malware to evade detection	Port redirector
Create implementation plan			Determine domain and IP address space	Identify job postings and needs/gaps	Dumpster dive	Identify vulnerabilities in third-party software libraries		Assess vulnerability of 3rd party vendors	Compromise 3rd party infrastructure to support delivery	Create backup infrastructure	Obtain Apple iOS enterprise distribution key pair and certificate	Create infected removable media	Test physical access	Upload, install, an configure software/tools
Create strategic plan			Determine external network trust dependencies	Identify people of interest	Identify business processes/tempo	Research relevant vulnerabilities/CVEs			Data Hiding	Domain registration hijacking		Discover new exploits and monitor exploit-provider forums	Test signature	
Derive intelligence requirements			Determine firmware version	Identify personnel with an authority/privilege	Identify business relationships	Research visibility gap of security vendors			DNSCalc	Dynamic DNS		Identify resources required to build capabilities		
				Identify sensitive personnel information	Identify job postings and needs/gaps							Obtain/re-use		
					Identify supply chains									
					Obtain									

Pre-ATT&CK Changes

- **New tactics**
- **Significant reduction in number of techniques**
- **Aiming to cover the scope of all current techniques that are**
  - a) technical
  - b) visible to some kind of defender
  - c) real

Mobile

Total Refresh

- New techniques
- Updating existing techniques
- New software entries to account for new threat reporting that we've identified,
- External contributions (and always looking for more!)
- Align more closely with Enterprise ATT&CK

Sub-Techniques

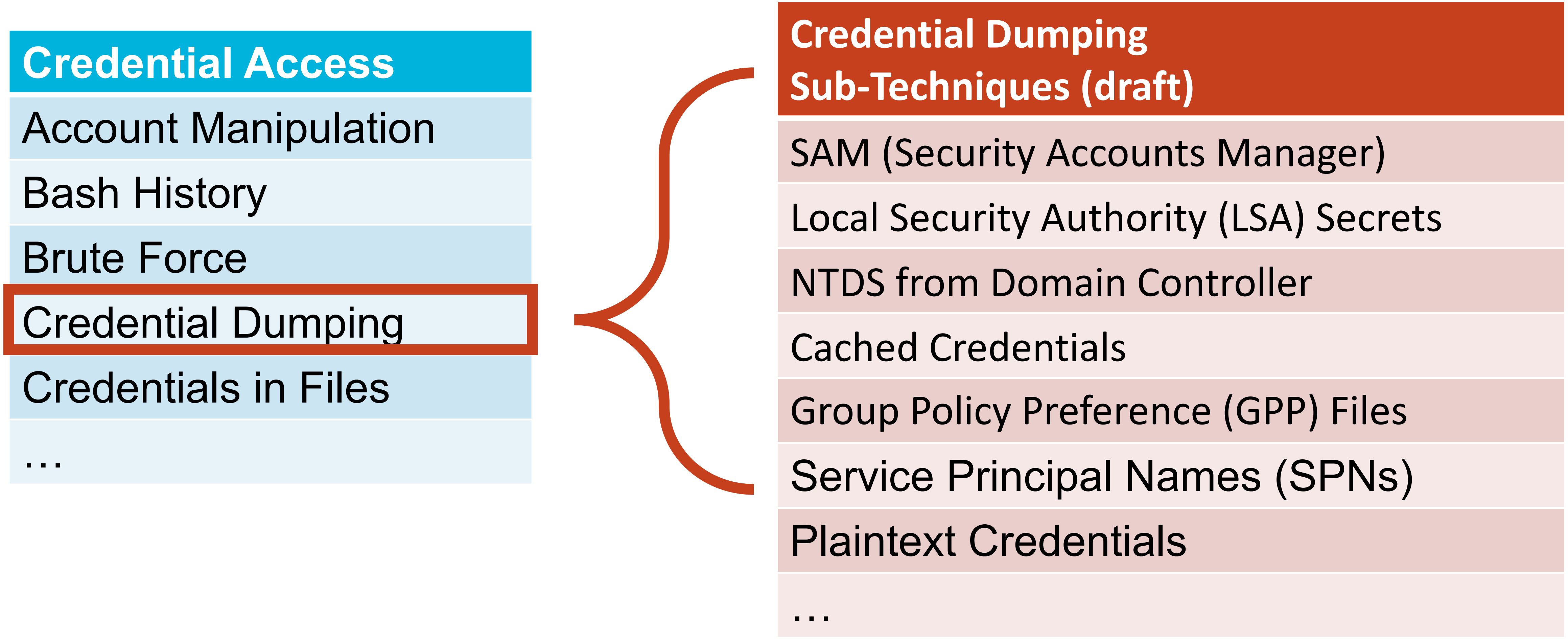
What are Sub-Techniques

- **Address differing levels of abstraction**
  - Consider example Execution techniques: **Scripting** vs. **Rundll32**
- **Major change for all ATT&CK users**

Credential Dumping Today

- In the description there 9 ways to perform the action
  - SAM (Security Accounts Manager)
  - Cached Credentials
  - Local Security Authority (LSA) Secrets
  - NTDS from Domain Controller
  - Group Policy Preference (GPP) Files
  - Service Principal Names (SPNs)
  - Plaintext Credentials
  - DCSync
  - Proc filesystem (Linux)
- **That’s a lot of different behaviors lumped into one technique even though the end result is similar each time**

Credential Dumping With Sub-techniques

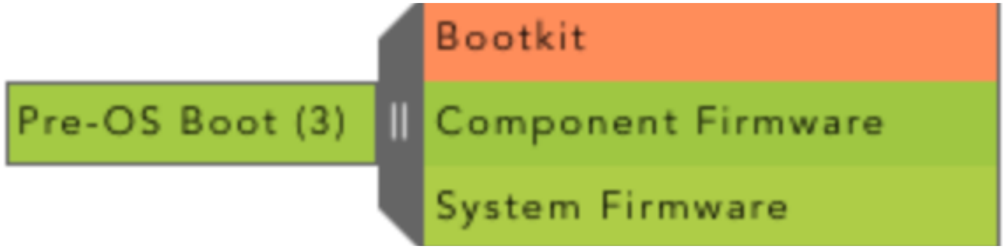


Credential Access
Account Manipulation
Bash History
Brute Force
Credential Dumping
Credentials in Files
…

Credential Dumping Sub-Techniques (draft)
SAM (Security Accounts Manager)
Local Security Authority (LSA) Secrets
NTDS from Domain Controller
Cached Credentials
Group Policy Preference (GPP) Files
Service Principal Names (SPNs)
Plaintext Credentials
…

How This Affects ATT&CK

- **New techniques** — We added a few new techniques to help us better organize sub-techniques. (Example: “Pre-OS Boot”)
- **Technique-to-sub-technique demotion** — We moved many techniques into sub-techniques. (Example: “Bootkit”)



How This Affects ATT&CK

- **New ID numbering**
  - T[technique].[sub-technique].
  - For example, Access Token Manipulation will still be T1134, but “Token Manipulation/Theft” will be T1134.001, “Create Process with Token” T1134.002, etc.

How This Affects ATT&CK

- **Technique decomposition** — Some techniques like Account Manipulation and Process Injection had several sub-techniques created from content in their previous definition.
- In other cases the techniques will get decomposed and sub-techniques will be assigned under other applicable techniques.
  - For example, Local Job Scheduling was decomposed into sub-techniques that fall under "Scheduled Task/Job" and "Scheduled Task/Job (Escalation Possible)".

How This Affects ATT&CK

- **Technique realignment and deprecation** — The analysis of techniques necessary to do sub-techniques led to some technique realignment between tactics and deprecation of techniques.
  - We pruned back several techniques that didn't fit the core definition of the tactic, like Hidden Files and Directories not fitting under Persistence,
  - and a small number that needed to be deprecated, like Hypervisor where we've found no documented use cases beyond proof of concepts.

Benefits

- Top-level techniques will change less frequently
- Coverage assessment
  - understand that there’s several ways a technique can be performed.
- Lead to more refined data sources that apply to techniques and sub-techniques on specific platforms.
- Provide a structure for others to add their own local sub-techniques under existing techniques to meet their specific requirements.
- Make it easier to fit the ATT&CK Matrix with techniques on a single slide. (Look, we make a lot of PowerPoints, and we know you do too!)

When is this happening?

- End of 2019
- Update will be in the form of a separate website to give people time to adjust and give us feedback before it becomes the "official" version of ATT&CK (3ish months post release).
- We want feedback from ATT&CK users to make sure we aren’t doing this in vain.
  - Please reach out to us at attack@mitre.org (Use a subject line that starts with “Sub-technique feedback” so it’s easy to spot.)

How Will This Affect Me?

- **Detections and Tooling**
  - review and refine
    - Many sub-techniques will map directly to “old” techniques, so in those cases you should only have to update IDs.
    - You will have some level of effort with mapping new techniques and sub-techniques as well as determining how to assign things like detection analytics to those sub-techniques that have been decomposed.

How Will This Affect Me?

- **Mapping Intel**
  - Significant change and level of effort
  - We plan to keep the historical site and STIX objects available as a reference for older intel that is mapped to the prior, pre-sub-technique version of ATT&CK.
  - Historic repositories
    - consider how you may want to approach that (e.g. only map new intel to the new ATT&CK version).
  - We are working on a tool to help with this but still expect this to be time consuming

Controls

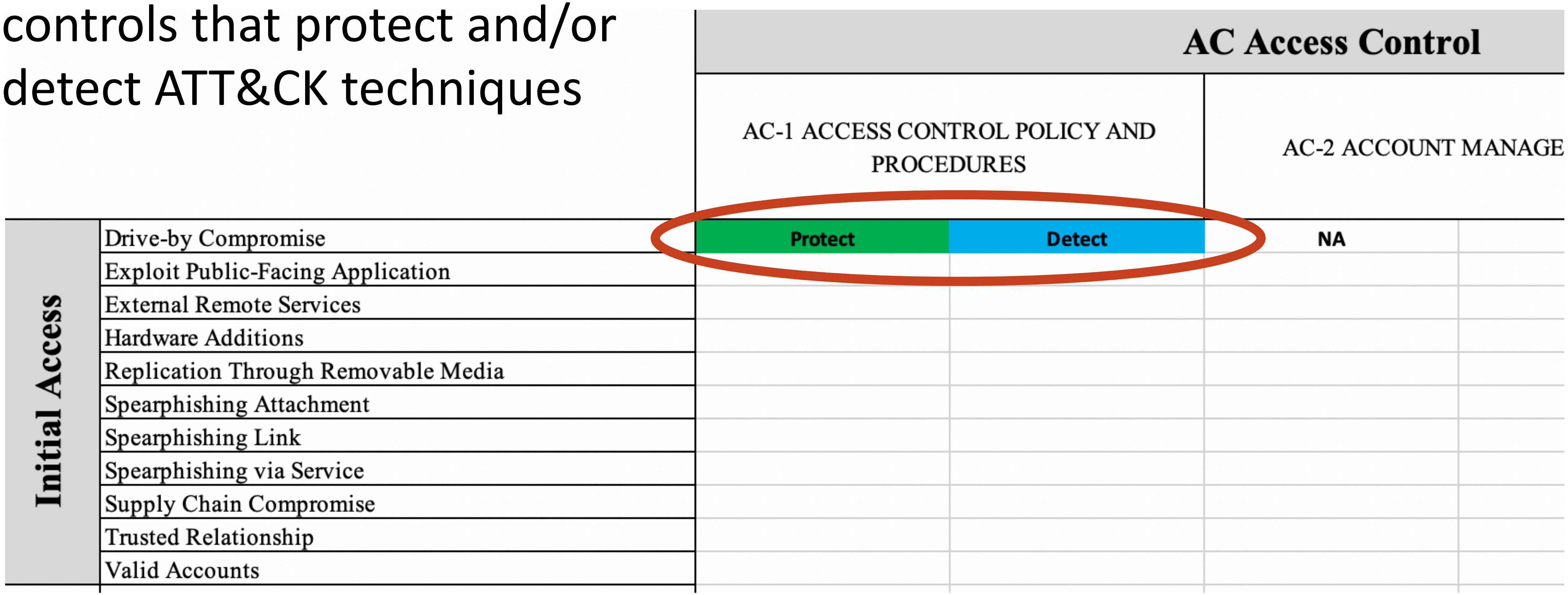
ATT&CK to NIST 800-53

- The task is extremely labor intensive due to the scope (314 ATT&CK techniques by 256 controls)
- Releasing a template mapping at ATT&CKcon 2019
- MITRE will crowd source the mapping so that it can be maintained collaboratively by the people who use it

Template Example

Mapping shows NIST 800-53 controls that protect and/or detect ATT&CK techniques

← NIST CONTROLS →



		AC Access Control			
		AC-1 ACCESS CONTROL POLICY AND PROCEDURES		AC-2 ACCOUNT MANAGE	
Initial Access	Drive-by Compromise	Protect	Detect	NA	
	Exploit Public-Facing Application				
	External Remote Services				
	Hardware Additions				
	Replication Through Removable Media				
	Spearphishing Attachment				
	Spearphishing Link				
	Spearphishing via Service				
	Supply Chain Compromise				
	Trusted Relationship				
	Valid Accounts				

← ATT&CK →

Cloud

Cloud

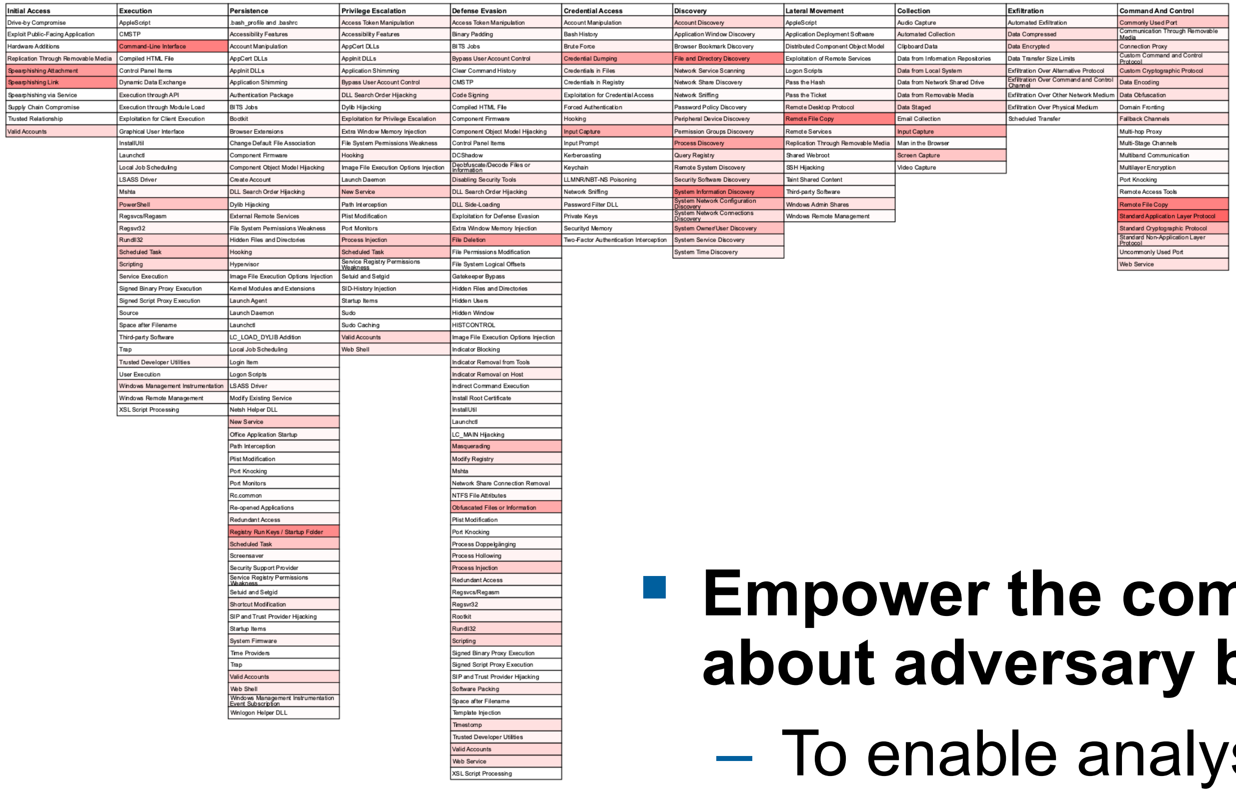
- First version of techniques going out in October with another big release happening next year.
- Cloud will be part of enterprise and will be represented by new platforms in addition to Windows/MacOS/Linux
- We’ve added three infrastructure as a service (IaaS) platforms:
  - Amazon Web Services (AWS),
  - Microsoft Azure (Azure), and
  - Google Cloud Platform (GCP).

Cloud (continued)

- The Software as a service (SaaS) platform will cover techniques against general cloud-based software platforms.
- Separately from IaaS and SaaS, we've also added two cloud software platforms to cover techniques against those specific platforms:
  - Azure Active Directory (Azure AD) and
  - Office 365
- 36 techniques have been added or updated to cover adversary behavior against cloud-based platforms.

ATT&CK Sightings

ATT&CK Sightings Ecosystem

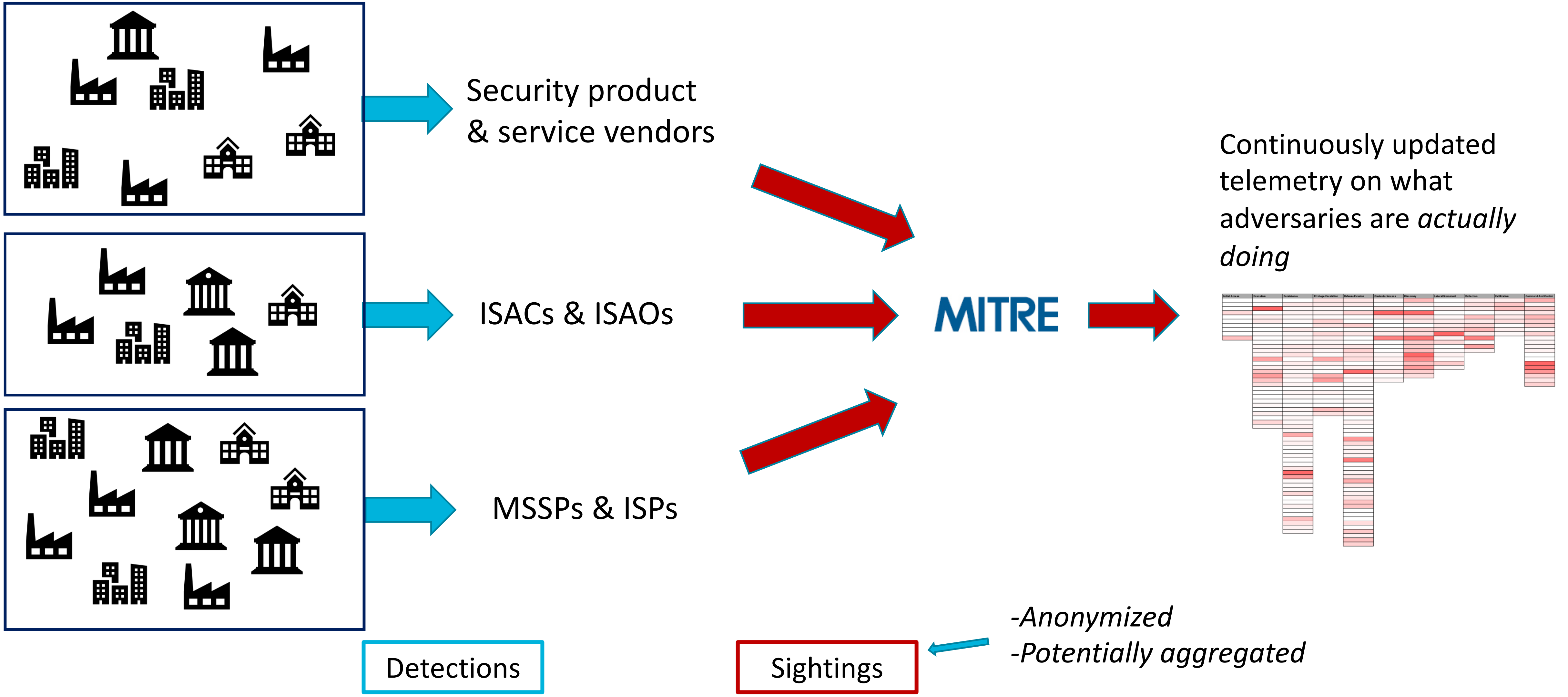


Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account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

- **Sighting: A detection of a specific adversary behavior as defined within ATT&CK**
  - **Example:** On 6/12/19, T1193 (Spearphishing Attachment) was detected in the US Financial Sector

- **Empower the community with real, anonymized data about adversary behavior from many sources**
  - To enable analysis of what adversaries are doing:
    - What techniques are being detected in the wild?
    - Are there differences in detections across different sectors?
    - How do behaviors change over time?

Vision of Desired End-State



Security product & service vendors

ISACs & ISAOs

MSSPs & ISPs

MITRE

Continuously updated telemetry on what adversaries are *actually doing*

Detections

Sightings

-Anonymized
-Potentially aggregated

Cyber Analytics Repository

Cyber Analytics Repository (CAR) Relaunch

- **Knowledge base of analytics developed by MITRE *based on* ATT&CK**
- **Relaunch goal was to address barriers**
  - Make it easy to contribute and use
- **Other updates**
  - Additions to process data model
  - New analytics
  - Native Splunk queries

ATT&CKcon 2.0

ATT&CKcon 2.0 October 29-30

Entire conference will be live-streamed!

Register at: https://www.mitre.org/attackcon-streamed-live

“Getting Started with ATT&CK™”

New eBook available at:

https://www.mitre.org/sites/default/files/publications/mitre-getting-started-with-attack-october-2019.pdf

ATT&CK

https://attack.mitre.org

attack@mitre.org

🐦 @MITREattack

rjs@mitre.org

MITRE

MITRE’s mission-driven teams are dedicated to solving problems for a safer world. Through our federally funded R&D centers and public-private partnerships, we work across government to tackle challenges to the safety, stability, and well-being of our nation.

Learn more www.mitre.org