Update from the MITRE ATT&CK Team

Adam Pennington
@_whatshisface

@MITREattack

MITRE

System Owner/User Discovery (T1033)

adamp$ whoami

- New Lead of MITRE ATT&CK
- 12 years with MITRE
- Focused on threat intel and deception
- Past defender and CTI analyst
- Part of ATT&CK since it was a spreadsheet with no &
- 11 years at Carnegie Mellon as student and researcher
- Certified decompression and rebreather diver
- Former live sound engineer

ATT&CK

MITRE

ATTACK Circa 2014

Persistence	Privilege Escalation	Credential Access	Host Enumeration	Defense Evasion	Lateral Movement	Command and Control	Exfiltration
New service	Exploitation of vulnerability	OS/Software Weakness	Process enumeration	Software packing	RDP	Common protocol, follows standard	Normal C&C channel
Modify existing service	Service file permissions weakness	User interaction	Service enumeration	Masquerading	Windows admin shares (C$, ADMIN$)	Common protocol, non-standard	Alternate data channel
DLL Proxying	Service registry permissions weakness	Network sniffing	Local network config	DLL Injection	Windows shared webroot	Commonly used protocol on non-standard port	Exfiltration over other network medium
Hypervisor Rookit	DLL path hijacking	Stored file	Local network connections	DLL loading	Remote vulnerability	Communications encrypted	Exfiltration over physical medium
Winlogon Helper DLL	Path interception		Window enumeration	Standard protocols	Logon scripts	Communications are obfuscated	Encrypted separately
Path Interception	Modification of shortcuts		Account enumeration	Obfuscated payload	Application deployment software	Distributed communications	Compressed separately
Registry run keys / Startup folder addition	Editing of default handlers		Group enumeration		Taint shared content	Multiple protocols combined	Data staged
Modification of shortcuts	AT / Schtasks / Cron		Owner/user enumeration		Access to remote services with valid credentials		Automated or scripted data exfiltration
MBR / BIOS rootkit			Operating system enumeration		Pass the hash		Size limits
Editing of default handlers			Security software enumeration				
AT / Schtasks / Cron			File system enumeration				

ATT&CK

MITRE

Enterprise ATT&CK as of May 2020

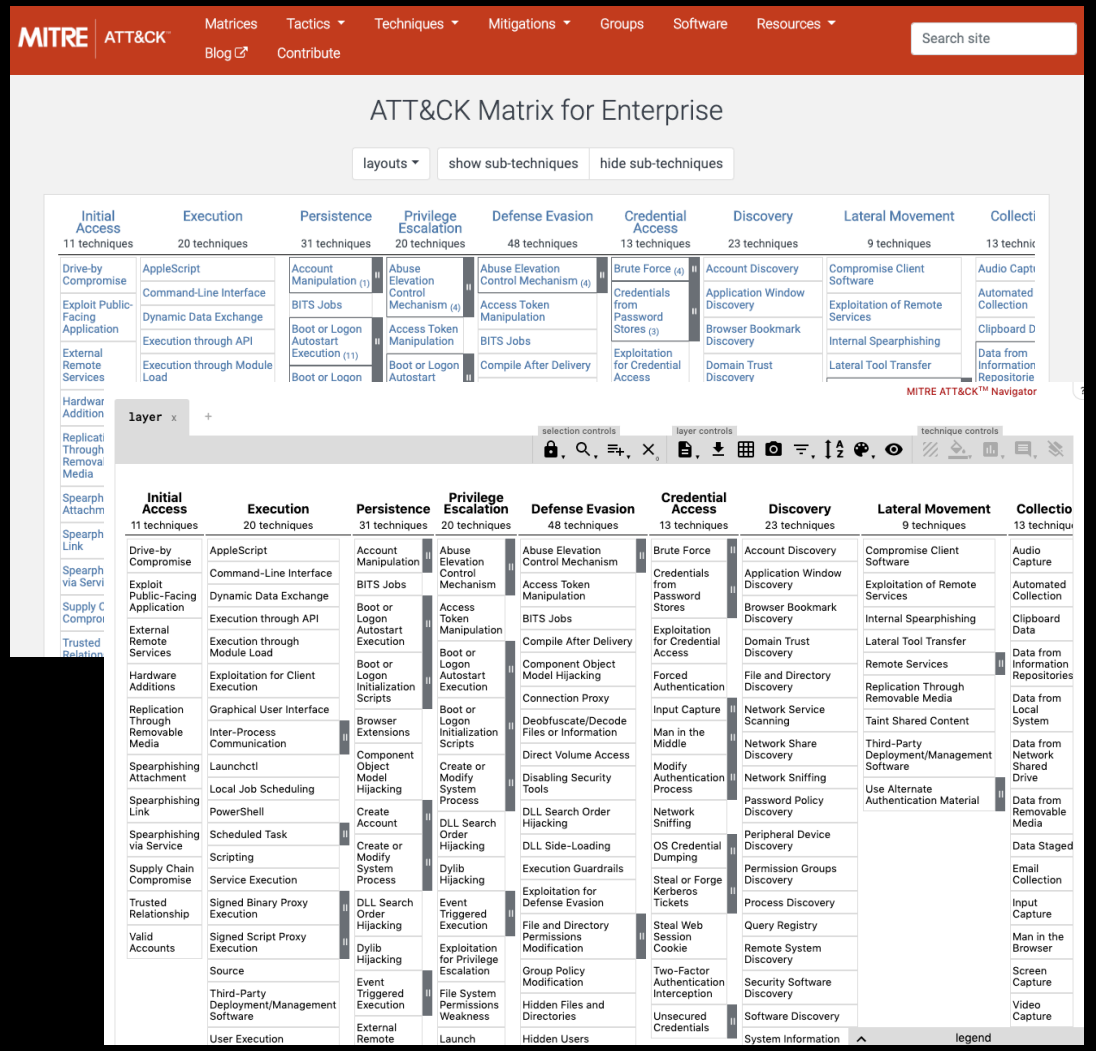
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	Scheduled Task			Binary Padding	Network Sniffing		AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration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

Issues with ATT&CK in 2020

- **Technique abstraction imbalance across knowledge base**
  - Some techniques broad: Masquerading
  - Some techniques narrow: Rundll32
  - Most common complaint over the past couple of years
- **Techniques have a lot of depth to them**
  - Some don’t read beyond the name
  - An analytic per technique may not make coverage “green”
- **Technique overload**
  - Too many techniques!
  - The matrix is too big!

Our Solution: Sub-Techniques

- **Released March 31st in beta**
  - Website
  - STIX 2.0 (Not yet via TAXII)
  - ATT&CK Navigator
  - Crosswalks from pre sub-techniques to sub-techniques
  - Design & Philosophy paper



ATT&CK with Sub-Techniques Beta

Initial Access 9 techniques	Execution 10 techniques	Persistence 17 techniques	Privilege Escalation 12 techniques	Defense Evasion 32 techniques	Credential Access 13 techniques	Discovery 21 techniques	Lateral Movement 9 techniques	Collection 15 techniques	Command and Control 16 techniques	Exfiltration 8 techniques	Impact 13 techniques
Drive-by Compromise	Command and Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Brute Force	Account Discovery	Exploitation of Remote Services	Archive Collected Data	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Credentials from Password Stores	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
External Remote Services	Inter-Process Communication	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Hardware Additions	Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information	Forced Authentication	Domain Trust Discovery	Remote Service Session Hijacking	Clipboard Data	Data Obfuscation	Exfiltration Over C2 Channel	Data Manipulation
Phishing	Scheduled Task/Job	Browser Extensions	Create or Modify System Process	Direct Volume Access	Input Capture	File and Directory Discovery	Remote Services	Data from Information Repositories	Dynamic Resolution	Exfiltration Over Other Network Medium	Defacement
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution	Execution Guardrails	Man-in-the-Middle	Network Service Scanning	Replication Through Removable Media	Data from Local System	Encrypted Channel	Exfiltration Over Physical Medium	Disk Wipe
Supply Chain Compromise	Software Deployment Tools	Create Account	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Modify Authentication Process	Network Share Discovery	Software Deployment Tools	Data from Network Shared Drive	Fallback Channels	Exfiltration Over Web Service	Endpoint Denial of Service
Trusted Relationship	System Services	Create or Modify System Process	Group Policy Modification	File and Directory Permissions Modification	Network Sniffing	Network Sniffing	Taint Shared Content	Data from Removable Media	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Valid Accounts	User Execution	Event Triggered Execution	Hijack Execution Flow	Group Policy Modification	OS Credential Dumping	Password Policy Discovery	Use Alternate Authentication Material	Data Staged	Multi-Stage Channels		Inhibit System Recovery
	Windows Management Instrumentation	External Remote Services	Process Injection	Hide Artifacts	Steal or Forge Kerberos Tickets	Peripheral Device Discovery		Email Collection	Non-Application Layer Protocol		Network Denial of Service
		Hijack Execution Flow	Scheduled Task/Job	Hijack Execution Flow	Steal Web Session Cookie	Permission Groups Discovery		Input Capture	Non-Standard Port		Resource Hijacking
		Office Application Startup	Valid Accounts	Impair Defenses	Two-Factor Authentication Interception	Process Discovery		Man in the Browser	Protocol Tunneling		Service Stop
		Pre-OS Boot		Indicator Removal on Host	Unsecured Credentials	Query Registry		Man-in-the-Middle	Proxy		System Shutdown/Reboot
		Scheduled Task/Job		Indirect Command Execution		Remote System Discovery		Screen Capture	Remote Access Software		
		Server Software Component		Masquerading		Software Discovery		Video Capture	Traffic Signaling		
		Traffic Signaling		Modify Authentication Process		System Information Discovery			Web Service		
		Valid Accounts		Modify Registry		System Network Configuration Discovery					
				Obfuscated Files or Information		System Network Connections Discovery					
				Pre-OS Boot		System Owner/User Discovery					
				Process Injection		System Service Discovery					
				Rogue Domain Controller		System Time Discovery					
				Rootkit							
				Signed Binary Proxy Execution							
				Signed Script Proxy Execution							
				Subvert Trust Controls							
				Template Injection							
				Traffic Signaling							
				Trusted Developer Utilities Proxy Execution							
				Use Alternate Authentication Material							
				Valid Accounts							
				Virtualization/Sandbox Evasion							
				XSL Script Processing							

ATT&CK

MITRE

What is a Sub-Technique?

- **It's a more specific technique**
  - Still describes behavior, but at a lower level
  - Still intelligence driven, observed in the wild use

- **Sub-techniques are <u>not</u> procedures!**
  - Procedures continue to be specific adversary implementation

- **Sub-technique Initial coverage**
  - Enterprise
  - Cloud

ATT&CK®

MITRE

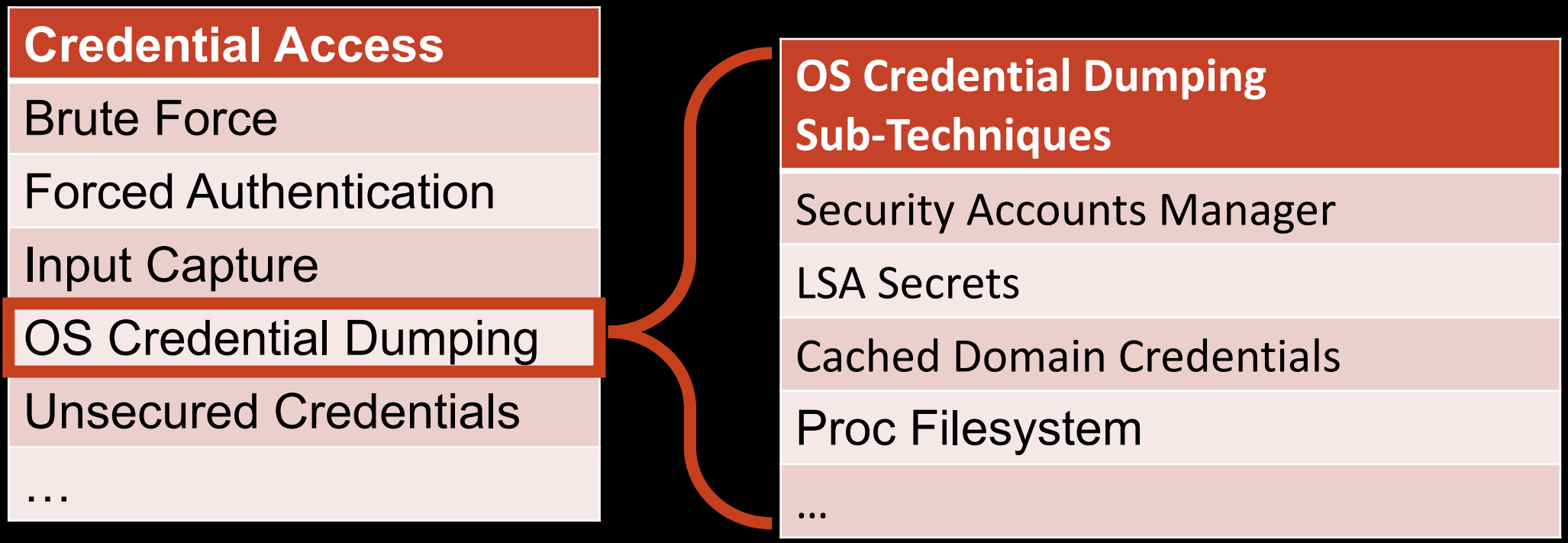
What Do Sub-Techniques Mean for ATT&CK?

- **Large reorganization of information**
  - Initial release is same data, just new structure
- **Fixes a lot of the abstraction issues**
- **More sustainable growth**
  - Reduction by 99 techniques
  - Provides better framework for others to add to local copies
- **Easier to convey complexity of techniques for coverage**
- **Opportunity to trim/refine**
  - Several techniques deprecated: hypervisor, etc.
  - Higher level ideas broken out: masquerading

ATT&CK

MITRE

Sub-Technique Example



ATT&CK

MITRE

New Technique Page – Pre-OS Boot

Home > Techniques > Enterprise > Pre-OS Boot

Pre-OS Boot

Sub-techniques (3)

ID	Name
T1542.001	System Firmware
T1542.002	Component Firmware
T1542.003	Bootkit

Adversaries may abuse Pre-OS Boot mechanisms as a way to establish persistence on a system. During the booting process of a computer, firmware and various startup services are loaded before the operating system. These programs control flow of execution before the operating system takes control.[1]

Adversaries may overwrite data in boot drivers or firmware such as BIOS (Basic Input/Output System) and The Unified Extensible Firmware Interface (UEFI) to persist on systems at a layer below the operating system. This can be particularly difficult to detect as malware at this level will not be detected by host software-based defenses.

ID: T1542

Sub-techniques: T1542.001, T1542.002, T1542.003

Tactic: Defense Evasion, Persistence

Platform: Linux, Windows

Permissions Required: Administrator, SYSTEM

Data Sources: VBR, MBR, Component firmware, Process monitoring, Disk forensics, EFI, BIOS, API monitoring

Defense Bypassed: Anti-virus, Host intrusion prevention systems, File monitoring

Version: 1.0

Mitigations

Mitigation	Description
Boot Integrity	Use Trusted Platform Module technology and a secure or trusted boot process to prevent system integrity from being compromised. Check the integrity of the existing BIOS or EFI to determine if it is vulnerable to modification. [2] [3]
Privileged Account Management	Ensure proper permissions are in place to help prevent adversary access to privileged accounts necessary to perform these actions
Update Software	Patch the BIOS and EFI as necessary.

Detection

Perform integrity checking on pre-OS boot mechanisms that can be manipulated for malicious purposes. Take snapshots of boot records and firmware and compare against known good images. Log changes to boot records, BIOS, and EFI, which can be performed by API calls, and compare against known good behavior and patching.

Disk check, forensic utilities, and data from device drivers (i.e. processes and API calls) may reveal anomalies that warrant deeper investigation. [4]

ATT&CK

MITRE

New Sub-Technique – System Firmware

Home > Techniques > Enterprise > Pre-OS Boot > System Firmware (sub)

Pre-OS Boot: System Firmware

Other sub-techniques of Pre-OS Boot (3)

ID	Name
T1542.001	System Firmware
T1542.002	Component Firmware
T1542.003	Bootkit

The BIOS (Basic Input/Output System) and The Unified Extensible Firmware Interface (UEFI) or Extensible Firmware Interface (EFI) are examples of system firmware that operate as the software interface between the operating system and hardware of a computer. [1] [2] [3]

System firmware like BIOS and (U)EFI underly the functionality of a computer and may be modified by an adversary to perform or assist in malicious activity. Capabilities exist to overwrite the system firmware, which may give sophisticated adversaries a means to install malicious firmware updates as a means of persistence on a system that may be difficult to detect.

ID: T1542.001
Tactic: Persistence, Defense Evasion
Platform: Windows
Permissions Required: Administrator, SYSTEM
Data Sources: EFI, BIOS, API monitoring
Defense Bypassed: Host intrusion prevention systems, Anti-virus, File monitoring
CAPEC ID: capec-532
Contributors: McAfee; Ryan Becwar
Version: 1.0

Procedure Examples

Name	Description
Hacking Team UEFI Rootkit	Hacking Team UEFI Rootkit is a UEFI BIOS rootkit developed by the company Hacking Team to persist remote access software on some targeted systems.[5]
LoJax	LoJax is a UEFI BIOS rootkit deployed to persist remote access software on some targeted systems.[6]
Trojan.Mebromi	Trojan.Mebromi performs BIOS modification and can download and execute a file as well as protect itself from removal.[7]

Mitigations

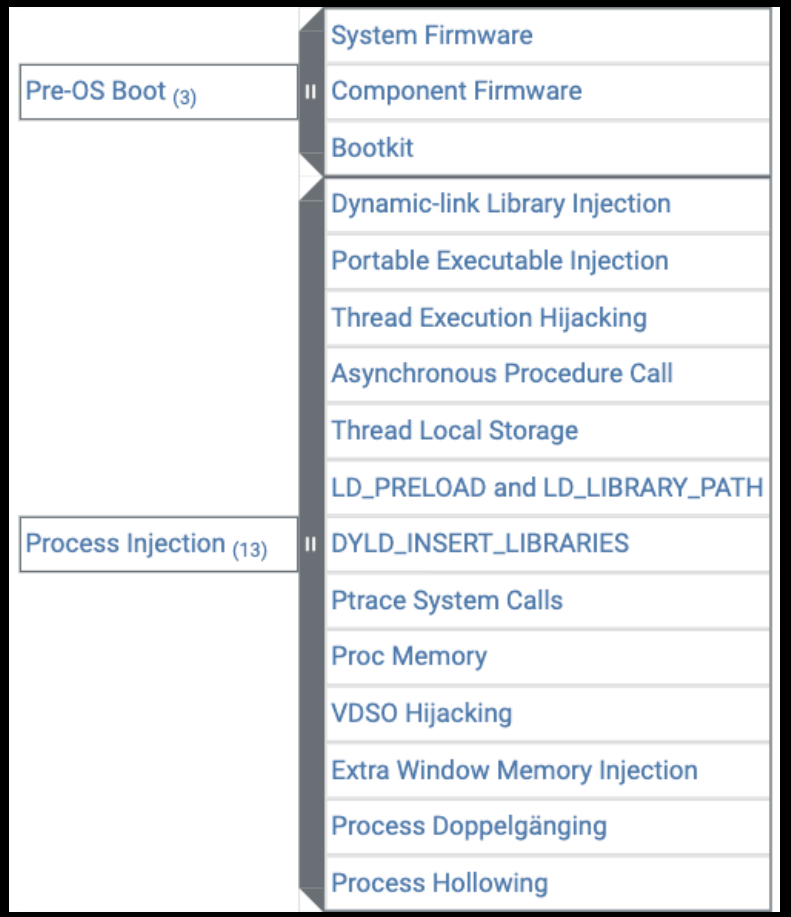
Mitigation	Description
Boot Integrity	Check the integrity of the existing BIOS or EFI to determine if it is vulnerable to modification. Use Trusted Platform Module technology. [4]
Privileged Account Management	Prevent adversary access to privileged accounts or access necessary to perform this technique.
Update Software	Patch the BIOS and EFI as necessary.

ATT&CK

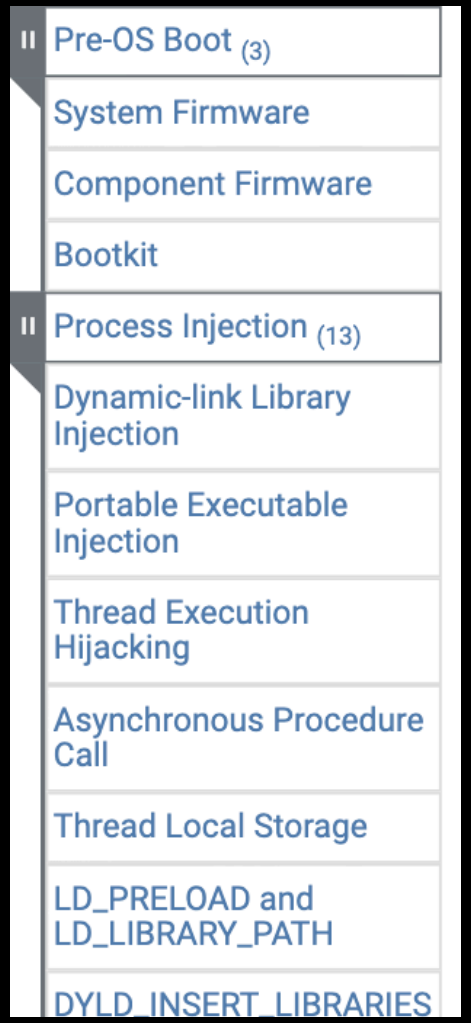
MITRE

New Matrix Visualizations

Side Layout



Flat Layout



Things You Should Know About Subs

- **ID Structure: T####.### - T[technique].[sub-technique]**
  - e.g. Pre-OS Boot: **T1542**; System Firmware: **T1542.001**

- **Single parent from sub-techniques to technique**
- **Sub-techniques *may* have different tactics within a technique**
- **Not all techniques have a sub-technique**

- **Procedures mapped to sub-techniques where possible**
  - Ambiguous info goes to technique

ATT&CK

MITRE

Timeline for Sub-Techniques

- **Beta of sub-techniques released March 31, 2020**
  - Currently in feedback/review period
  - Feedback has been largely positive
- **Accepting contributions for techniques/groups/software**
  - Will **only** be updating sub-technique version of ATT&CK
- **On track for an early July 2020 release**

Other Sub-Technique Information Resources

- **Sub-technique update log**
  - https://attack.mitre.org/beta/resources/updates/updates-march-2020/index.html
- **Old ATT&CK to sub-technique crosswalk files:**
  - CSV: https://attack.mitre.org/docs/subtechniques/subtechniques-csv.zip
  - JSON: https://attack.mitre.org/docs/subtechniques/subtechniques-crosswalk.json
- **Updated ATT&CK Design and Philosophy paper:**
  - https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf
- **ATT&CK mitre/cti GitHub repo for JSON STIX content:**
  - https://github.com/mitre/cti/tree/subtechniques
- **ATT&CK Navigator sub-technique beta**
  - https://mitre-attack.github.io/attack-navigator/beta/

On Deck After Sub-Techniques

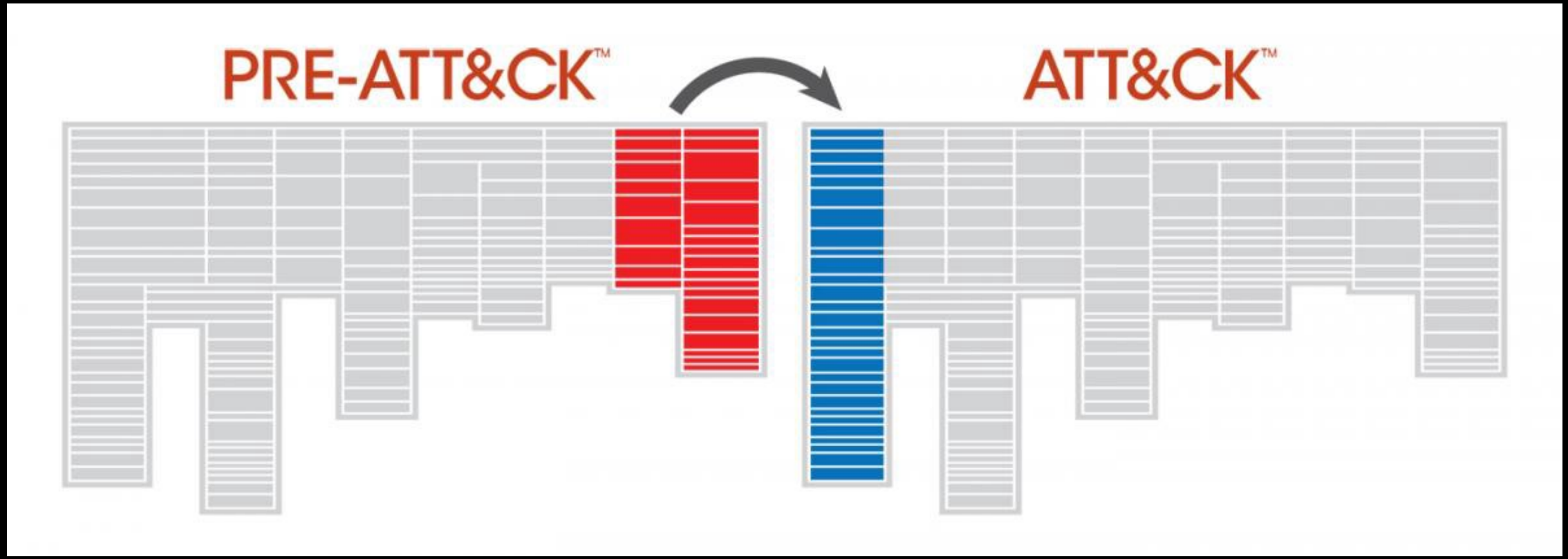
Mobile ATT&CK

Enterprise ATT&CK

PRE-ATT&CK

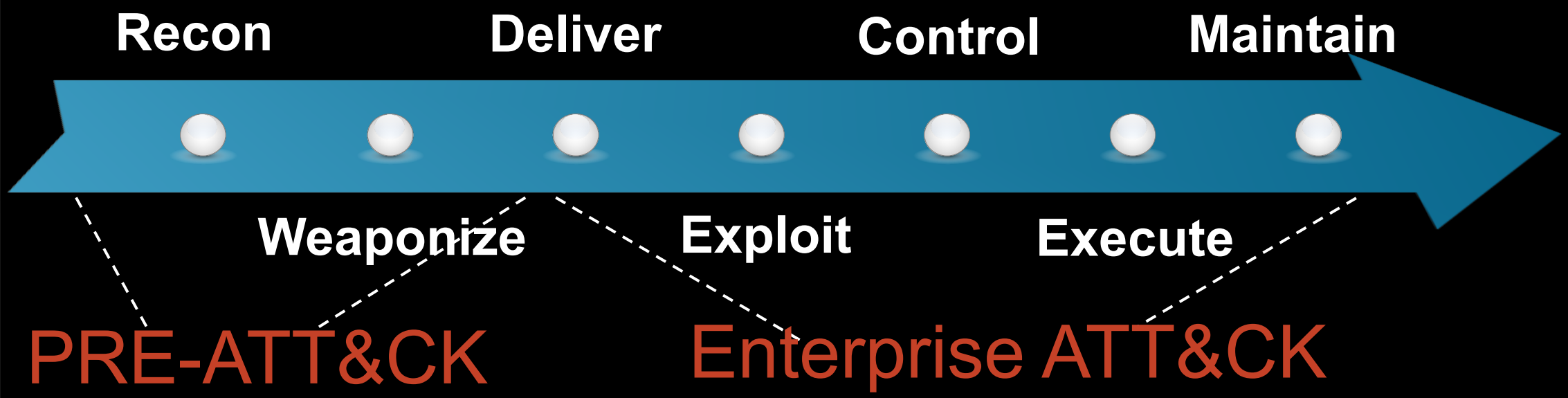
It's just ATT&CK

Launch/Compromise -> Initial Access

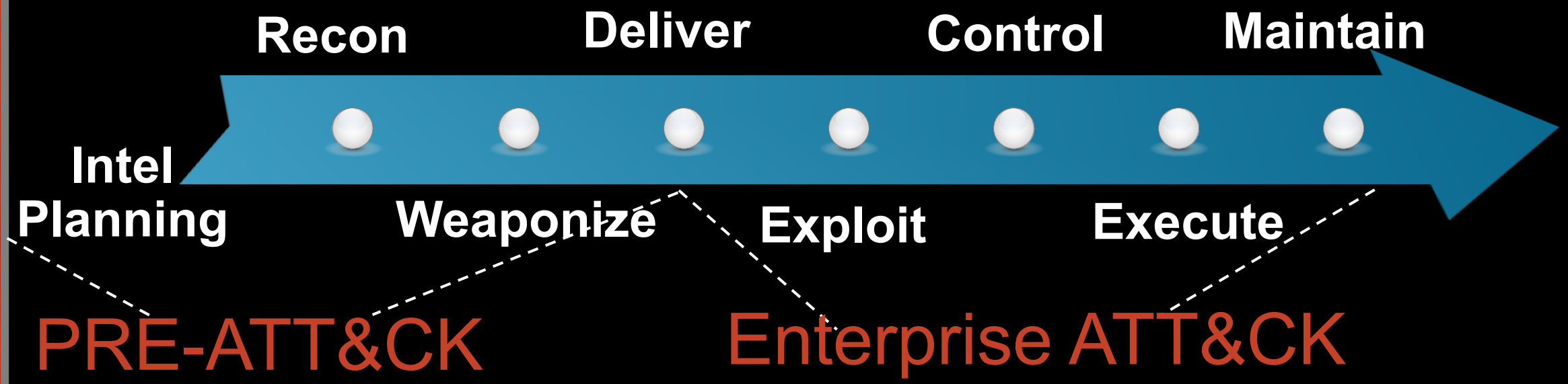


2018

PRE's Place in the Adversary Lifecycle



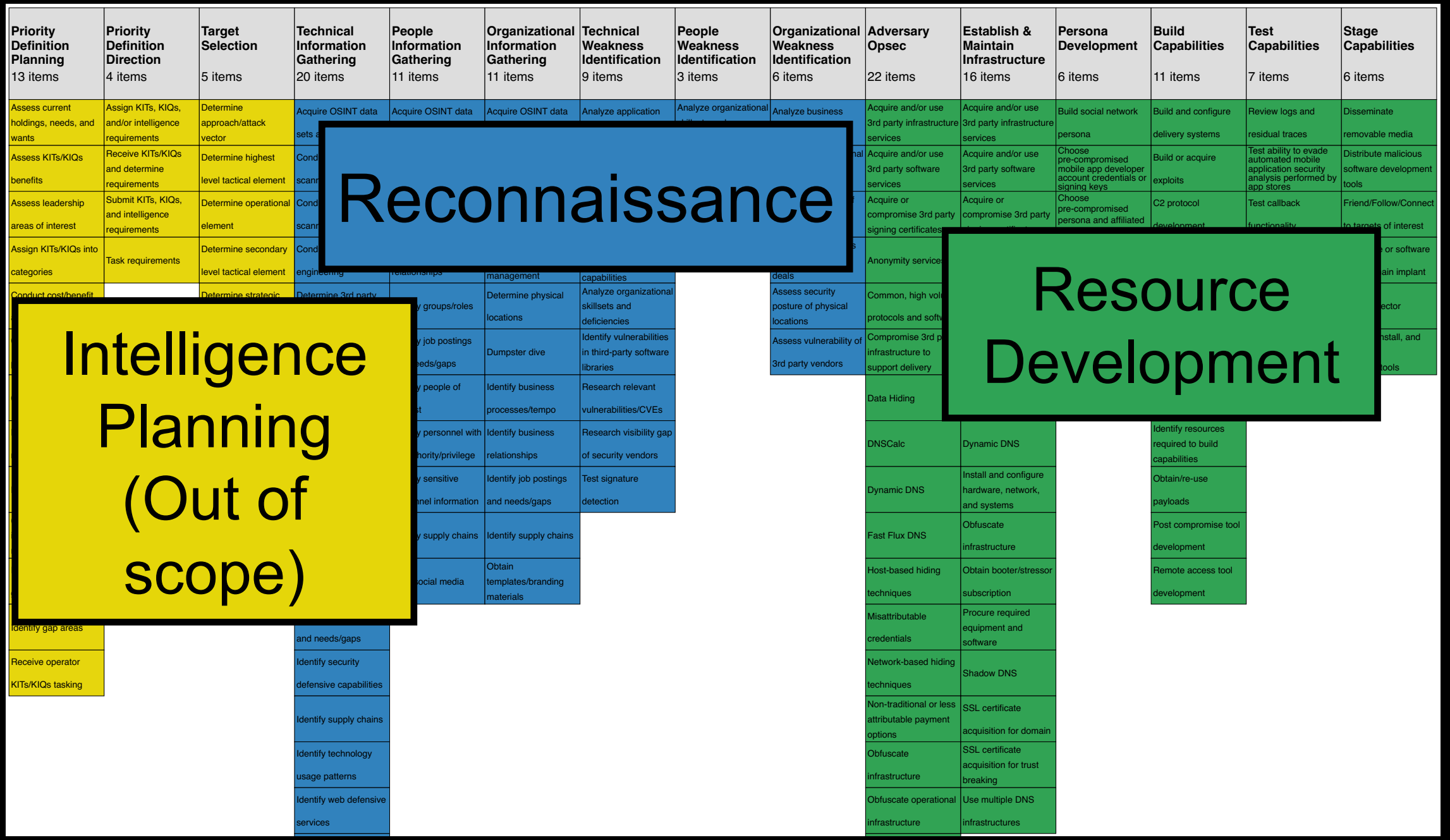
PRE's Place in the Adversary Lifecycle



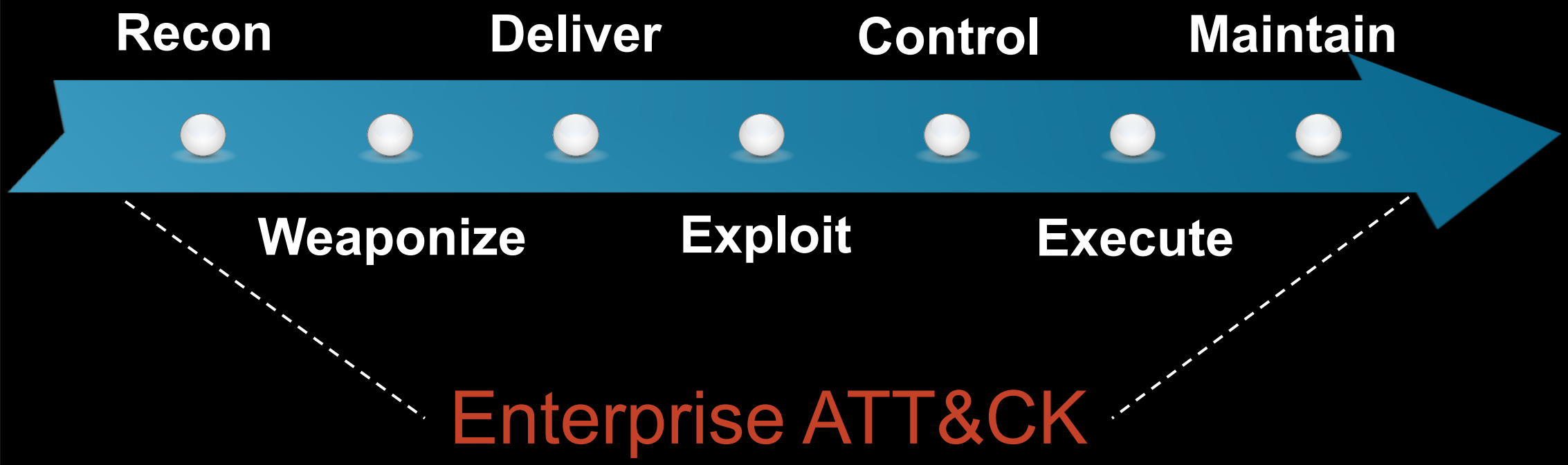
How do we scope techniques?

- Technical
- Visible to some defenders
- Evidence of adversary use

Priority Definition Planning 13 items	Priority Definition Direction 4 items	Target Selection 5 items	Technical Information Gathering 20 items	People Information Gathering 11 items	Organizational Information Gathering 11 items	Technical Weakness Identification 9 items	People Weakness Identification 3 items	Organizational Weakness Identification 6 items	Adversary Opsec 22 items	Establish & Maintain Infrastructure 16 items	Persona Development 6 items	Build Capabilities 11 items	Test Capabilities 7 items	Stage Capabilities 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 removable 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 malicious software development 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/Connect to targets of interest
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 software supply chain implant
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, and 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 detection for file upload/email filters	
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		
Develop KITs/KIQs			Discover target logon/email address format	Identify sensitive personnel information	Identify job postings and needs/gaps	Test signature detection			Dynamic DNS	Install and configure hardware, network, and systems		Obtain/re-use payloads		
Generate analyst intelligence requirements			Enumerate client configurations	Identify supply chains	Identify supply chains				Fast Flux DNS	Obfuscate infrastructure		Post compromise tool development		
Identify analyst level gaps			Enumerate externally facing software applications technologies, languages, and dependencies	Mine social media	Obtain templates/branding materials				Host-based hiding techniques	Obtain booter/stressor subscription		Remote access tool development		
Identify gap areas			Identify job postings and needs/gaps						Misattributable credentials	Procure required equipment and software				
Receive operator KITs/KIQs tasking			Identify security defensive capabilities						Network-based hiding techniques	Shadow DNS				
			Identify supply chains						Non-traditional or less attributable payment options	SSL certificate acquisition for domain				
			Identify technology usage patterns						Obfuscate infrastructure	SSL certificate acquisition for trust breaking				
			Identify web defensive services						Obfuscate operational infrastructure	Use multiple DNS infrastructures				



Post-Merger Enterprise ATT&CK



PRE-ATT&CK Merger Roadmap

- **Reconnaissance and Resource Development tactics**
  - Technique development ongoing
  - Next release after sub-techniques
  - Currently slated for August 2020

- **Looking at how to preserve the content of PRE-ATT&CK**
  - We've heard from people using "intel planning" for teaching
  - Open to input

Other Upcoming ATT&CK Plans

- **Revamp of ATT&CK data sources**
  - Planned initial release of source definitions to GitHub
- **Technique coverage of network devices such as routers**
- **New ATT&CK training on defense and analytics**
  - Continue training series that started with CTI in January

ATT&CK To

ATT&CK Sightings

ATT&CK Evaluations

PRE-ATT&CK

ATT&CK for ICS

Mobile ATT&CK

ATT&CK-Based SOC Assessments

Cyber Analytics Repository

ATT&CK Updates this Past Year

1 NEW TACTIC

43 NEW TECHNIQUES

13 NEW MOBILE TECHNIQUES

16 NEW GROUPS

87 NEW SOFTWARE

41 NEW MITIGATIONS

87 UPDATED TECHNIQUES

16 UPDATED MOB TECHNIQUES

67 UPDATED GROUPS

92 UPDATED SOFTWARE

ATT&CK for ICS – Released in Jan

Unique Adversary Goals

Technology Differences

Different Defenses

ATT&CK

MITRE

MITRE | ATT&CK™ for Cloud

Credit to Dave Herrald and Ryan Kovar

ATT&CK for Cloud

- **36 techniques**
- **Part of Enterprise ATT&CK**
- **Almost 100% community-contributed techniques!**
  - Input from:
    - A cloud service provider
    - Red teams
    - Threat analysts
    - Detection analysts

Google Cloud

Azure Active Directory

ATT&CK

MITRE

ATT&CK

MITRE

Impact Tactic

- Attacks targeting availability and integrity
  - Ex: Ransomware, DoS, destruction
- 16 techniques

Data Destruction	Endpoint DoS	Resource Hijacking	Runtime Data Manipulation
Data Encrypted for Impact	Network DoS	Service Stop	Stored Data Manipulation
Disk Content Wipe	Firmware Corruption	Defacement	Transmitted Data Manipulation
Disk Structure Wipe	Inhibit System Recovery	System Shutdown/Reboot	Account Access Removal

MITRE

Mitigations as an Object

Home > Techniques > Enterprise > Spearphishing Attachment

Mitigations

Mitigation	Description
Antivirus/Antimalware	Anti-virus can also automatically quarantine suspicious files.
Network Intrusion Prevention	Network intrusion prevention systems and systems designed to scan and remove malicious email attachments can be used to block activity.
Restrict Web-Based Content	Block unknown or unused attachments by default that should not be transmitted over email as a best practice to prevent some vectors, such as .scr, .exe, .pif, .cpl, etc. Some email scanning devices can open and analyze compressed and encrypted formats, such as zip and rar that may be used to conceal malicious attachments in Obfuscated Files or Information.
User Training	Users can be trained to identify social engineering techniques and spearphishing emails.

MITRE

Other ATT&CK Team Talks

- **Today at 1830 CET/12:30 PM EDT**
  - ATT&CK Navigator Layer Scripts – Caleb Little
- **Today at 1845 CET/12:45 PM EDT**
  - Technique Report ATT&CK Mapper: TRAM – Connor Magee
- **Tomorrow at 1415 CET/8:15 AM EDT**
  - Bro/Zeek ATT&CK-based Analytics and Reporting: BZAR Mark Fernandez

Thank you to the ATT&CK Community

Individuals + orgs contributing to ATT&CK!

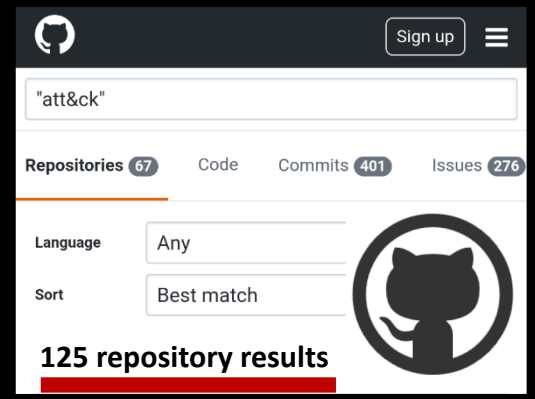
- Alain Homewood, Insomnia Security
- Alan Neville, @abnev
- Alex Hinchliffe, Palo Alto Networks
- Alfredo Abarca
- Allen DeRyke, ICE
- Anastasios Pingios
- Andrew Smith, @jakx_
- Avneet Singh
- Barry Shteiman, Exabeam
- Bart Parys
- Bartosz Jerzman
- Brian Prange
- Bryan Lee
- Carlos Borges, @huntingneo, CIP
- Casey Smith
- Christiaan Beek, @ChristiaanBeek
- Christoffer Strömblad
- Cody Thomas, SpecterOps
- Craig Aitchison
- CrowdStrike Falcon OverWatch
- Cybereason Nocturnus, @nocturnus
- Daniel Oakley
- Darren Spruell
- Dave Westgard
- David Ferguson, CyberSponse
- David Lu, Tripwire
- David Routin
- Drew Church, Splunk
- Ed Williams, Trustwave, SpiderLabs
- Edward Millington
- Elger Vinicius S. Rodrigues, CYBINT Centre
- Elia Florio, Microsoft
- Elly Searle, CrowdStrike
- Emily Ratliff, IBM
- ENDGAME
- Eric Kuehn, Secure Ideas
- Erika Noerenberg, @gutterchurl, Carbon Black
- Erye Hernandez, Palo Alto Networks
- ESET
- Felipe Espósito, @Pr0teus
- Filip Kafka, ESET
- FS-ISAC
- Hans Christoffer Gaardløs
- Heather Linn
- Itamar Mizrahi
- Itzik Kotler, SafeBreach
- Ivan Sinyakov
- Jacob Wilkin, Trustwave, SpiderLabs
- Jan Miller, CrowdStrike
- Jannie Li, Microsoft (MSTIC)
- Jared Atkinson, @jaredcatkinson
- Jean-Ian Boutin, ESET
- Jeff Sakowicz, Microsoft (IDPM Services)
- Jeremy Galloway
- Jimmy Astle, @AstleJimmy, Carbon Black
- Johann Rehberger
- John Lambert, Microsoft (MSTIC)
- John Strand
- Josh Abraham
- Justin Warner, ICEBRG
- Jörg Abraham, EclecticIQ
- Kaspersky
- Lab52 by S2 Grupo
- Leo Loobeek, @leoloobeek
- Loic Jaquemet
- Lucas da Silva Pereira, @vulcanunsec, CIP
- Lukáš Štefanko, ESET
- Marc-Etienne M.Léveillé, ESET
- Mark Wee
- Martin Jirkal, ESET
- Martin Smolar, ESET
- Matias Nicolas Porolli, ESET
- Matt Graeber, @mattifestation, SpecterOps
- Matt Kelly, @breakersall
- Matthew Demaske, Adaptforward
- Matthew Molyett, @s1air
- McAfee
- Michael Cox
- Michal Dida, ESET
- Microsoft Threat Intelligence Center (MSTIC)
- Mike Kemmerer
- Milos Stojadinovic
- Mnemonic
- Netskope
- Nick Carr, FireEye
- Nik Seetharaman, Palantir
- Nishan Maharjan, @loki248
- Oddvar Moe, @oddvarmoe
- Oleg Kolesnikov
- Oleg Skulkin, Group-IB
- Omkar Gudhate
- Patrick Campbell, @pjcampbe11
- Paul Speulstra, AECOM
- Pedro Harrison
- Praetorian
- Prashant Verma, Paladion
- Rahmat Nurfauzi, PT Xynexis International
- Red Canary
- RedHuntLabs, @redhuntlabs
- Ricardo Dias
- Richard Gold, Digital Shadows
- Richie Cyrus, SpecterOps
- Rob Smith
- Robby Winchester, @robwinchester3
- Robert Falcone
- Romain Dumont, ESET
- Ryan Becwar
- Ryan Benson, Exabeam
- Sahar Shukrun
- Saisha Agrawal, Microsoft (MSTIC)
- Scott Lundgren, @5twenty9, Carbon Black
- Shailesh Tiwary (Indian Army)
- Shane Tully, @securitygypsy
- Stefan Kanthak
- Sudhanshu Chauhan, @Sudhanshu_C
- Sunny Neo
- Swetha Prabakaran, Microsoft (MSTIC)
- Sylvain Gil, Exabeam
- Tatsuya Daitoku, Cyber Defense Institute, Inc.
- Teodor Cimpoesu
- Tim MalcomVetter
- Tom Ueltschi @c_APT_ure
- Tony Lambert, Red Canary
- Travis Smith, Tripwire
- Tristan Bennett, Seamless Intelligence
- Valerii Marchuk, Cybersecurity Help s.r.o.
- Veeral Patel
- Vincent Le Toux
- Walker Johnson
- Wayne Silva, Countercept
- Ye Yint Min Thu Htut, DBS Bank
- Yonatan Gotlib, Deep Instinct

ATT&CK
@MITREattack

MITRE ATT&CK™ - A knowledge base for describing behavior of adversaries across their lifecycle (Replying/Following/Re-tweeting ≠ endorsement)

McLean, VA attack.mitre.org
Joined May 2015

491 Following **33.1K** Followers



Adam Pennington
@_whatshisface

ATT&CK®

attack@mitre.org
@MITREattack

MITRE