

Detecting the Adversary Post-Compromise with Threat Models and Behavioral Analytics

Approved for Public Release; Distribution Unlimited. 16-3058
© 2016 The MITRE Corporation. All rights reserved.

Cyber Attack Lifecycle

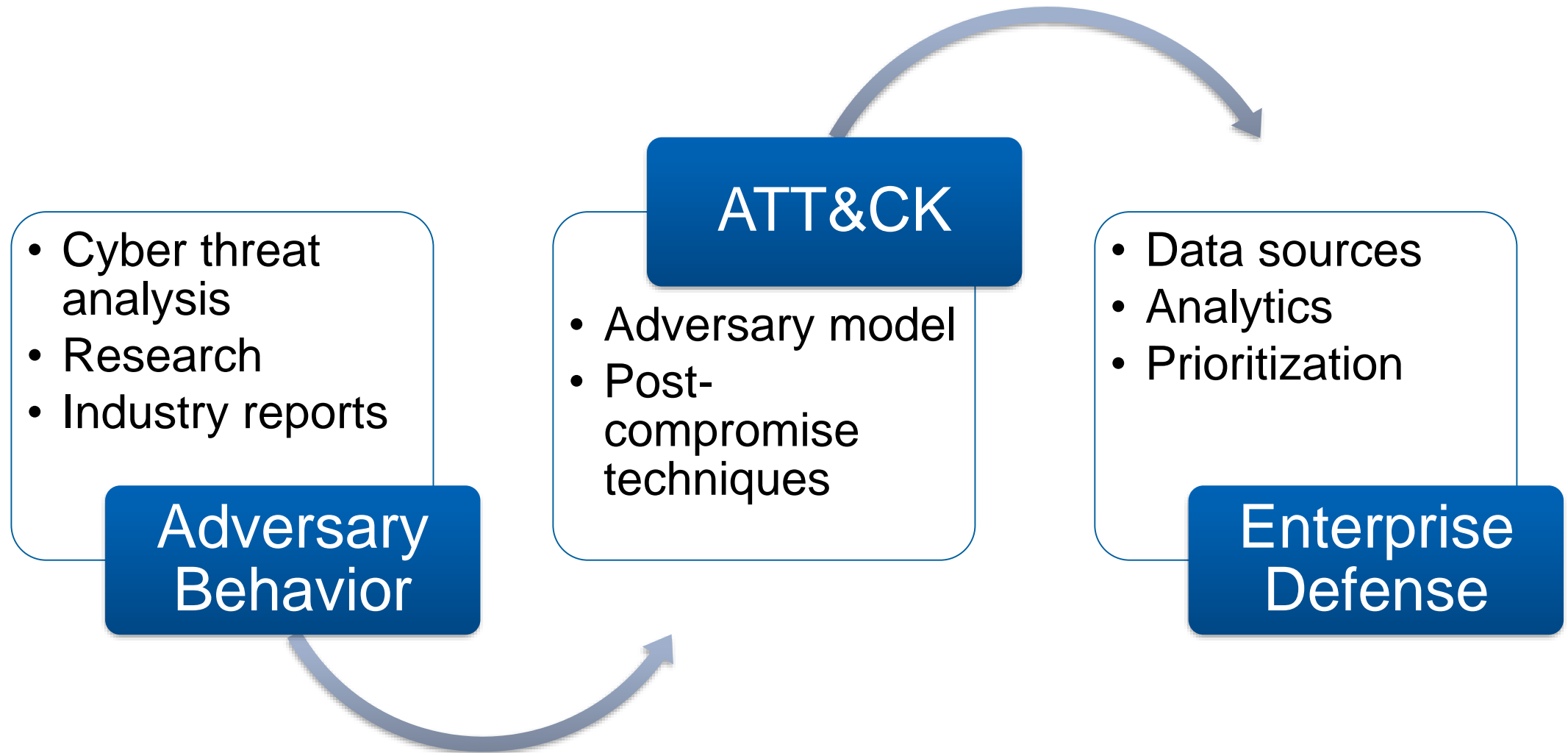


146 days - The median time an adversary is in a network before being detected

-Mandiant, M-Trends 2016



Threat Based Modeling



ATT&CK: Deconstructing the Lifecycle



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

Threat data informed adversary model

Higher fidelity on right-of-exploit, post-access phases

Describes behavior sans adversary tools

Working with world-class researchers to improve and expand

ATT&CK Matrix Tactics and Techniques (2014)

Persistence	Privilege Escalation	Credential Access	Host Enumeration	Defense Evasion	Lateral Movement	Command and Control	Exfiltration
New service	Exploitation of vulnerability	Credential dumping	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	Indicator removal	Taint shared content	Multiple protocols combined	Data staged
Modification of shortcuts	Scheduled task		Owner/user enumeration	Indicator blocking	Access to remote services with valid credentials		Automated or scripted data exfiltration
MBR / BIOS rootkit	Legitimate Credentials		Operating system enumeration		Pass the hash		Size limits
Editing of default handlers			Security software enumeration				Scheduled transfer
Scheduled task			File system enumeration				

ATT&CK Matrix Tactics and Techniques (2015)

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Host Enumeration	Lateral Movement	Execution	C2	Exfiltration		
Legitimate Credentials			Credential Dumping	Account enumeration	Application deployment software	Command Line	Commonly used port	Automated or scripted exfiltration		
Accessibility Features		File system enumeration		Exploitation of Vulnerability	Logon scripts	File Access			Comm through removable media	
AddMonitor	Binary Padding DLL Side-Loading Disabling Security Tools File System Logical Offsets Process Hollowing Rootkit		Credentials in Files			Group permission enumeration	Pass the hash	PowerShell		Custom application layer
DLL Search Order Hijack		Network Sniffing	Local network connection enumeration	Pass the ticket	Process Hollowing	protocol	encrypted Data size limits			
Edit Default File Handlers		User Interaction		Peer connections	Registry	Custom encryption cipher	Data staged			
New Service		Credential manipulation	Local networking enumeration	Remote Desktop Protocol	Scheduled Task	obfuscation	Exfil over C2 channel			
Path Interception					Service Manipulation	Fallback channels	Exfil over alternate channel to C2 network			
Scheduled Task		Indicator blocking on host Indicator removal from tools Indicator removal from host Masquerading NTFS Extended Attributes Obfuscated Payload Rundll32 Scripting Software Packing Timestamp	Operating system enumeration	Windows management instrumentation	Third Party Software	Multiband comm	Exfil over other network medium			
Service File Permission Weakness						Windows remote management	Multilayer encryption	Peer connections	Standard app layer protocol	Exfil over physical medium
Shortcut Modification										
Web shell						Taint shared content	Standard encryption cipher	From network resource		
BIOS									Uncommonly used port	Scheduled transfer
Hypervisor Rootkit	Windows admin shares									
Logon Scripts										
Master Boot Record										
Mod. Exist'g Service										
Registry Run Keys										
Serv. Reg. Perm. Weakness										
Windows Mgmt Instr. Event Subsc.										
Winlogon Helper DLL										

ATT&CK Matrix Tactics and Techniques (2016)

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	
New Service		DLL Side-Loading	Credentials in Files	Local Network Configuration Discovery		InstallUtil	Data from Removable Media	Exfiltration Over Command and Control Channel	Custom Cryptographic Protocol
Path Interception		Disabling Security Tools	Input Capture		Logon Scripts	PowerShell			
Scheduled Task		File Deletion	Network Sniffing	Local Network Connections Discovery	Pass the Hash	Process Hollowing	Exfiltration Over Other Network Medium	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				Indicator Blocking	Peripheral Device Discovery	Network Service Scanning	Remote Desktop Protocol	Regsvr32	Exfiltration Over Physical Medium
Web Shell		Permission Groups Discovery	Remote File Copy			Rundll32	Screen Capture	Multiband Communication	
Basic Input/Output System	Exploitation of Vulnerability			Remote Services	Scheduled Task	Scripting	Exfiltration Over Physical Medium	Multilayer Encryption	
	Bypass User Account Control								Replication Through Removable Media
Bootkit	DLL Injection			Process Discovery	Shared Webroot	Windows Management Instrumentation	Scheduled Transfer	Remote File Copy	
Change Default File Association		Indicator Removal from Tools	Query Registry						Taint Shared Content
Component Firmware		Indicator Removal on Host		Remote System Discovery	Windows Admin Shares	Standard Cryptographic Protocol			
Hypervisor			InstallUtil				Security Software Discovery	Standard Non-Application Layer Protocol	
Logon Scripts		Masquerading		System Information Discovery	Uncommonly Used Port				
Modify Existing Service			Modify Registry			System Owner/User Discovery	Web Service		
Redundant Access		NTFS Extended Attributes		System Service Discovery	Web Service				
Registry Run Keys / Start Folder			Obfuscated Files or Information			System Service Discovery	Web Service		
Security Support Provider		Process Hollowing		System Service Discovery	Web Service				
Shortcut Modification			Redundant Access			System Service Discovery	Web Service		
Windows Management Instrumentation Event Subscription		Regsvcs/Regasm		System Service Discovery	Web Service				
		Regsvr32	System Service Discovery			Web Service			
		Rootkit		System Service Discovery	Web Service				
		Rundll32	System Service Discovery			Web Service			
Scripting		System Service Discovery		Web Service					
Software Packing			System Service Discovery		Web Service				
Timestamp		System Service Discovery		Web Service					

The ATT&CK Model

- **Consists of:**
 1. Tactic phases derived from Cyber Attack Lifecycle
 2. List of techniques available to adversaries for each phase
 3. Possible methods of detection and mitigation
 4. Documented adversary use of techniques and software
 5. Disambiguation of adversary names

- **Publically available adversary information is a problem**
 - Not granular enough
 - Insufficient volume



Image source: US Army

<http://www.flickr.com/photos/35703177@N00/3102597630/>

Mr. Potato Head is a registered trademark of Hasbro Inc.

Example of Technique Details – Persistence: New Service

- **Description:** When operating systems boot up, they can start programs or applications called services that perform background system functions. ... Adversaries may install a new service which will be executed at startup by directly modifying the registry or by using tools.
- **Platform:** Windows
- **Permissions required:** Administrator, SYSTEM
- **Effective permissions:** SYSTEM
- **Detection:**
 - Monitor service creation through changes in the Registry and common utilities using command-line invocation
 - Tools such as Sysinternals Autoruns may be used to detect system changes that could be attempts at persistence
 - Monitor processes and command-line arguments for actions that could create services
- **Mitigation:**
 - Limit privileges of user accounts and remediate [Privilege Escalation](#) vectors
 - Identify and block unnecessary system utilities or potentially malicious software that may be used to create services
- **Data Sources:** Windows Registry, process monitoring, command-line parameters
- **Examples:** *Carbanak, Lazarus Group, TinyZBot, Duqu, CozyCar, CosmicDuke, hcdLoader, ...*
- **CAPEC ID:** [CAPEC-550](#)

Example of Group Details: Deep Panda

- **Description:** Deep Panda is a suspected Chinese threat group known to target many industries, including government, defense, financial, and telecommunications¹. The intrusion into healthcare company Anthem has been attributed to Deep Panda².
- **Aliases:** Deep Panda, Shell Crew, WebMasters, KungFu Kittens, PinkPanther, Black Vine
- **Techniques:**
 - [PowerShell](#)
 - [Windows Management Instrumentation](#)
 - [Web Shell](#)
 - [Windows Admin Shares](#)
 - [Process Discovery](#)
 - [Scripting](#)
 - [Indicator Removal from Tools](#)
 - [Regsvr32](#)
 - [Accessibility Features](#)
- **Software:** [Net](#), [Tasklist](#), [Sakula](#), [Mivast](#), [Derusbi](#)
- **References:**
 1. Alperovitch, D. (2014, July 7). [Deep in Thought: Chinese Targeting of National Security Think Tanks](#). Retrieved November 12, 2014.
 2. ThreatConnect Research Team. (2015, February 27). [The Anthem Hack: All Roads Lead to China](#). Retrieved January 26, 2016.

Example of Software Details: Tasklist

- **Description:** The Tasklist utility displays a list of applications and services with its Process ID (PID) for all tasks running on either a local or a remote computer. It is packaged with Windows operating systems and can be executed from the command line¹.
- **Aliases:** Tasklist
- **Type:** Tool
- **Windows builtin software:** Yes
- **Techniques Used:**
 - [Process Discovery](#): Tasklist can be used to discover processes running on a system.
 - [Security Software Discovery](#): Tasklist can be used to enumerate security software currently running on a system by process name of known products.
 - [System Service Discovery](#): Tasklist can be used to discover services running on a system.
- **Groups:** [Deep Panda](#), [Turla](#), [Naikon](#)
- **References:**
 1. Microsoft. (n.d.). [Tasklist](#). Retrieved December 23, 2015.

Use Cases

- **Gap analysis with current defenses**
 - How do we improve our security posture?
- **Prioritize detection/mitigation of heavily used techniques**
 - Given our architecture, what is our level of exposure to specific techniques and groups ?
- **Information sharing**
 - How can we share observed behaviors on our network among our analysts and partners ?
- **Track a specific adversary's set of techniques**
 - If there is a breach by a known group , how do we report on it and track TTP changes ?
- **Simulations, exercises**
 - How can we effectively test our defenses and analytics against threat behaviors ?
- **New technologies, research**
 - How do we find gaps in current defensive technology ?

Notional Defense Gaps

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	Custom Command and Control Protocol	
AppInit DLLs		Code Signing	File and Directory Discovery			Execution through API	Data from Local System		Data Transfer Size Limits
Local Port Monitor		Component Firmware		Exploitation of Vulnerability	Graphical User Interface		Data from Network Shared Drive	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
New Service		DLL Side-Loading	Local Network Configuration Discovery			PowerShell	Data from Removable Media	Exfiltration Over Command and Control Channel	
Path Interception		Disabling Security Tools	Input Capture	Logon Scripts	Process Hollowing	Email Collection	Exfiltration Over Other Network Medium	Data Obfuscation	
Scheduled Task		File Deletion	Network Sniffing	Pass the Hash	Regsvcs/Regasm			Fallback Channels	
Service File Permissions Weakness		File System Logical Offsets	Two-Factor Authentication Interception	Connections Discovery	Pass the Ticket	Input Capture	Exfiltration Over Physical Medium	Multi-Stage Channels	
Service Registry Permissions Weakness				Network Service Scanning	Remote Desktop Protocol	Regsvr32		Screen Capture	Multiband Communication
Web Shell		Indicator Blocking	Peripheral Device Discovery	Remote File Copy	Rundll32			Scheduled Transfer	Peer Connections
Basic Input/Output System	Exploitation of Vulnerability			Remote Services	Scheduled Task				Multilayer Encryption
	Bypass User Account Control			Permission Groups Discovery	Scripting				
Bootkit	DLL Injection			Process Discovery	Service Execution				
Change Default File Association		Indicator Removal from Tools		Query Registry	Shared Webroot	Standard Application Layer Protocol			
				Remote System Discovery	Taint Shared Content				
Component Firmware		Indicator Removal on Host		Windows Admin Shares	Standard Cryptographic Protocol				
Hypervisor		InstallUtil		Security Software Discovery					
Logon Scripts		Masquerading		System Information Discovery		Standard Non-Application Layer Protocol			
Modify Existing Service		Modify Registry		System Owner/User Discovery					
Redundant Access		NTFS Extended Attributes		System Service Discovery					
Registry Run Keys / Start Folder		Obfuscated Files or Information							
Security Support Provider		Process Hollowing							
Shortcut Modification		Redundant Access							
Windows Management Instrumentation Event Subscription		Regsvcs/Regasm							
		Regsvr32							
Winlogon Helper DLL		Rootkit							
		Rundll32							
	Scripting								
	Software Packing								
	Timestamp								

High Confidence Med Confidence No Confidence

Adversary Visibility at the Perimeter

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	Custom Command and Control Protocol	
AppInit DLLs		Code Signing	File and Directory Discovery		Execution through API	Data from Local System	Data Transfer Size Limits		
Local Port Monitor		Component Firmware		Local Network Configuration Discovery	Exploitation of Vulnerability	Graphical User Interface	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
New Service		DLL Side-Loading	Credentials in Files		InstallUtil	Data from Removable Media	Exfiltration Over Command and Control Channel	Custom Cryptographic Protocol	
Path Interception		Disabling Security Tools	Input Capture	PowerShell					
Scheduled Task		File Deletion	Network Sniffing	Process Hollowing	Email Collection	Exfiltration Over Other Network Medium	Data Obfuscation		
Service File Permissions Weakness		File System Logical Offsets	Two-Factor Authentication Interception	Regsvcs/Regasm					
Service Registry Permissions Weakness					Network Service Scanning	Remote Desktop Protocol	Input Capture	Exfiltration Over Physical Medium	Fallback Channels
Web Shell		Indicator Blocking		Remote File Copy	Screen Capture	Scheduled Transfer	Multi-Stage Channels		
Basic Input/Output System	Exploitation of Vulnerability			Peripheral Device Discovery	Remote Services	Scheduled Task	Exfiltration Over Physical Medium	Multiband Communication	
	Bypass User Account Control		Permission Groups Discovery	Replication Through Removable Media	Scripting	Multilayer Encryption			
Bootkit	DLL Injection			Process Discovery	Shared Webroot	Service Execution	Scheduled Transfer	Peer Connections	
Change Default File Association		Indicator Removal from Tools		Query Registry	Taint Shared Content	Windows Management Instrumentation		Remote File Copy	
Component Firmware		Indicator Removal on Host	Remote System Discovery	Windows Admin Shares		Standard Application Layer Protocol			
Hypervisor		InstallUtil	Security Software Discovery			Standard Cryptographic Protocol			
Logon Scripts		Masquerading	System Information Discovery			Standard Non-Application Layer Protocol			
Modify Existing Service		Modify Registry	System Owner/User Discovery			Uncommonly Used Port			
Redundant Access		NTFS Extended Attributes	System Service Discovery			Web Service			
Registry Run Keys / Start Folder		Obfuscated Files or Information							
Security Support Provider		Process Hollowing							
Shortcut Modification		Redundant Access							
Windows Management Instrumentation Event Subscription		Regsvcs/Regasm							
Winlogon Helper DLL		Regsvr32							
		Rootkit							
		Rundll32							
		Scripting							
		Software Packing							
		Timestamp							
							High Confidence	Med Confidence	No Confidence

High Confidence Med Confidence No Confidence

Adversary Visibility at the Perimeter

- Adversary has the most latitude for variation at the network level
- Firewall, IDS/IPS, netflow, proxy, mail gateway, WCF, SSL MitM, protocol decoders, anomaly detection etc...
- All partial solutions
 - Don't add up to a complete one
- Often require specific prior knowledge
 - IPs, domains, malware changed easily
 - Sector, organization specific infrastructure
 - Frequently modify tools
 - Use legitimate channels
- Better coverage with host sensing

Defense Evasion	Exfiltration	Command and Control
DLL Search Order Hijacking	Automated Exfiltration	Commonly Used Port
Legitimate Credentials	Data Compressed	Communication Through Removable Media
Binary Padding	Data Encrypted	Custom Command and Control Protocol
Code Signing	Data Transfer Size Limits	Custom Cryptographic Protocol
Component Firmware	Exfiltration Over Alternative Protocol	Data Obfuscation
DLL Side-Loading	Exfiltration Over Command and Control Channel	Fallback Channels
Disabling Security Tools	Exfiltration Over Other Network Medium	Multi-Stage Channels
File Deletion	Exfiltration Over Physical Medium	Multiband Communication
File System Logical Offsets	Scheduled Transfer	Multilayer Encryption
Indicator Blocking		Peer Connections
Exploitation of Vulnerability		Remote File Copy
Bypass User Account Control		Standard Application Layer Protocol
DLL Injection		Standard Cryptographic Protocol
Indicator Removal from Tools		Standard Non-Application Layer Protocol
Indicator Removal on Host		Uncommonly Used Port
InstallUtil		Web Service
Masquerading		
Modify Registry		
NTFS Extended Attributes		
Obfuscated Files or Information		
Process Hollowing		
Redundant Access		
Regsvcs/Regasm		
Regsvr32		
Rootkit		
Rundll32		
Scripting		
Software Packing		
Timestamp		

+ Web Shell
(Persistence & Privilege Escalation)

Tactic Breakdown

Persistence

24

Lateral
Movement

14

Privilege
Escalation

14

Execution

15

Defense
Evasion

29

Collection

9

Credential
Access

8

Exfiltration

9

Discovery

15

Command
and Control

16

Publicly Known Adversary Use

Persistence	24	13	Lateral Movement	14	9
Privilege Escalation	14	10	Execution	15	9
Defense Evasion	29	26	Collection	9	9
Credential Access	8	8	Exfiltration	9	7
Discovery	15	15	Command and Control	16	16

Publically Reported Technique Use


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	Command-Line	Data Staged	Data Encrypted	
Appinit DLLs		Code Signing	Credential Manipulation	File and Directory Discovery	Software	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	Custom Cryptographic Protocol
New Service		DLL Side-Loading	Credentials in Files	Local Network	Logon Scripts	PowerShell	Data from Removable Media	Exfiltration Over Command and Control Channel	
Path Interception		Disabling Security Tools	Input Capture	Configuration Discovery	Pass the Hash	Process Hollowing			Data Obfuscation
Scheduled Task		File Deletion	Network Sniffing	Local Network Connections Discovery	Pass the Ticket	Regsvcs/Regasm	Email Collection		Fallback Channels
Service File Permissions Weakness		File System Logical Offsets	Two-Factor Authentication Interception	Network Service Scanning	Remote Desktop Protocol	Regsvr32	Input Capture	Exfiltration Over Other Network Medium	Multi-Stage Channels
Service Registry Permissions Weakness					Remote File Copy	Rundll32	Screen Capture		
Web Shell		Indicator Blocking		Peripheral Device Discovery	Remote Services	Scheduled Task		Exfiltration Over Physical Medium	Multiband Communication
Basic Input/Output System	Exploitation of Vulnerability			Permission Groups Discovery	Replication Through Removable Media	Scripting		Scheduled Transfer	Multilayer Encryption
Bootkit	Bypass User Account Control			Process Discovery	Shared Webroot	Service Execution			Peer Connections
Change Default File Association	DLL Injection			Query Registry	Taint Shared Content	Windows Management Instrumentation			Remote File Copy
Component Firmware		Indicator Removal from Tools		Remote System Discovery	Windows Admin Shares				Standard Application Layer Protocol
Hypervisor		Indicator Removal on Host		Security Software Discovery					Standard Cryptographic Protocol
Logon Scripts		InstallUtil		System Information Discovery					Standard Non-Application Layer Protocol
Modify Existing Service		Masquerading		System Owner/User Discovery					Uncommonly Used Port
Redundant Access		Modify Registry		System Service Discovery					Web Service
Registry Run Keys / Start Folder		NTFS Extended Attributes							
Security Support Provider		Obfuscated Files or Information							
Shortcut Modification		Process Hollowing							
Windows Management Instrumentation Event Subscription		Redundant Access							
Winlogon Helper DLL		Regsvcs/Regasm							
		Regsvr32							
		Rootkit							
		Rundll32							
		Scripting							
		Software Packing							
		Timestamp							

Public website – attack.mitre.org

[Log in](#)

[Page](#)
[Discussion](#)

[Read](#)
[View source](#)
[View history](#)



[Main page](#)
[Help](#)
[Contribute](#)
[References](#)
[Data Drilldown](#)

[Tactics](#)
[Persistence](#)
[Privilege Escalation](#)
[Defense Evasion](#)
[Credential Access](#)
[Discovery](#)
[Lateral Movement](#)
[Execution](#)
[Collection](#)
[Exfiltration](#)
[Command and Control](#)

[Techniques](#)
[All Techniques](#)
[Technique Matrix](#)

[Groups](#)
[All Groups](#)

[Software](#)
[All Software](#)

[Tools](#)
[Printable version](#)
[Permanent link](#)

[Follow @MITREattack](#)

Adversarial Tactics, Techniques & Common Knowledge

What's New

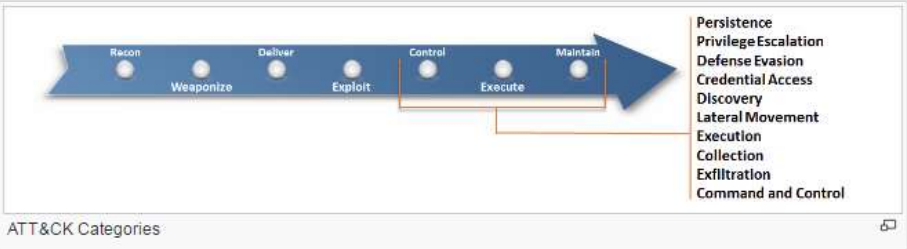
The July 2016 update includes a number of changes to the threat model and new features to the website:

- Expanded the tactics to ten with the inclusion of [Collection](#)
- Changed Host Enumeration to [Discovery](#)
- Expanded to 121 techniques from the original 96
- Enhanced the descriptions and information within many techniques
- Techniques can now be referenced by their technique ID in the site instead of by name
- Revamped the representation of threat Groups and the [Software](#) they use
- Added many new references to public threat reporting
- A subset of techniques now reference related attack pattern entries within CAPEC

Introduction

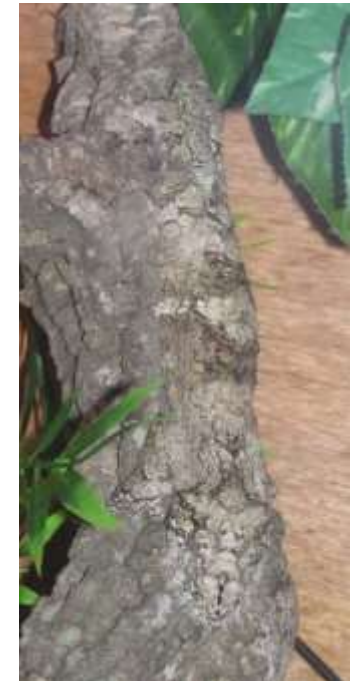
Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) is a model and framework for describing the actions an adversary may take while operating within an enterprise network. The model can be used to better characterize and describe post-compromise adversary behavior. It both expands the knowledge of network defenders and assists in prioritizing network defense by detailing the post-compromise (post-exploit and successful access) tactics, techniques, and procedures (TTPs) advanced persistent threats (APT) use to execute their objectives while operating inside a network.

ATT&CK incorporates information on cyber adversaries gathered through MITRE research, as well as from other disciplines such as penetration testing and red teaming to establish a collection of knowledge characterizing the post-compromise activities of adversaries. While there is significant research on initial exploitation and use of perimeter defenses, there is a gap in central knowledge of adversary process after initial access has been gained. ATT&CK focuses on TTPs adversaries use to make decisions, expand access, and execute their objectives. It aims to describe an adversary's steps at a high enough level to be applied widely across platforms, but still maintain enough details to be technically useful.



Defender's Problem: Adversaries Blend In

- **Attackers post-exploit look very similar to normal users**
- **Traditional efforts aren't effective at finding an active intrusion**
 - Internal tools look for compliance violations, exploits, or C2 channels
 - Indicator sharing only covers what's known and is fragile



Photos from Wikimedia Commons: https://commons.m.wikimedia.org/wiki/Camouflage_in_nature#

ATT&CK-Based Analytics Development Method

- **Post-compromise detection**
- **Focused on known behaviors**
- **Threat-based model**
- **Iterative by design**
- **Developed in a realistic environment**



Picture from: https://upload.wikimedia.org/wikipedia/commons/b/b7/Operating_a_Computer_Keyboard_MOD_45158105.jpg

Our Living Lab – The Fort Meade Experiment (FMX)

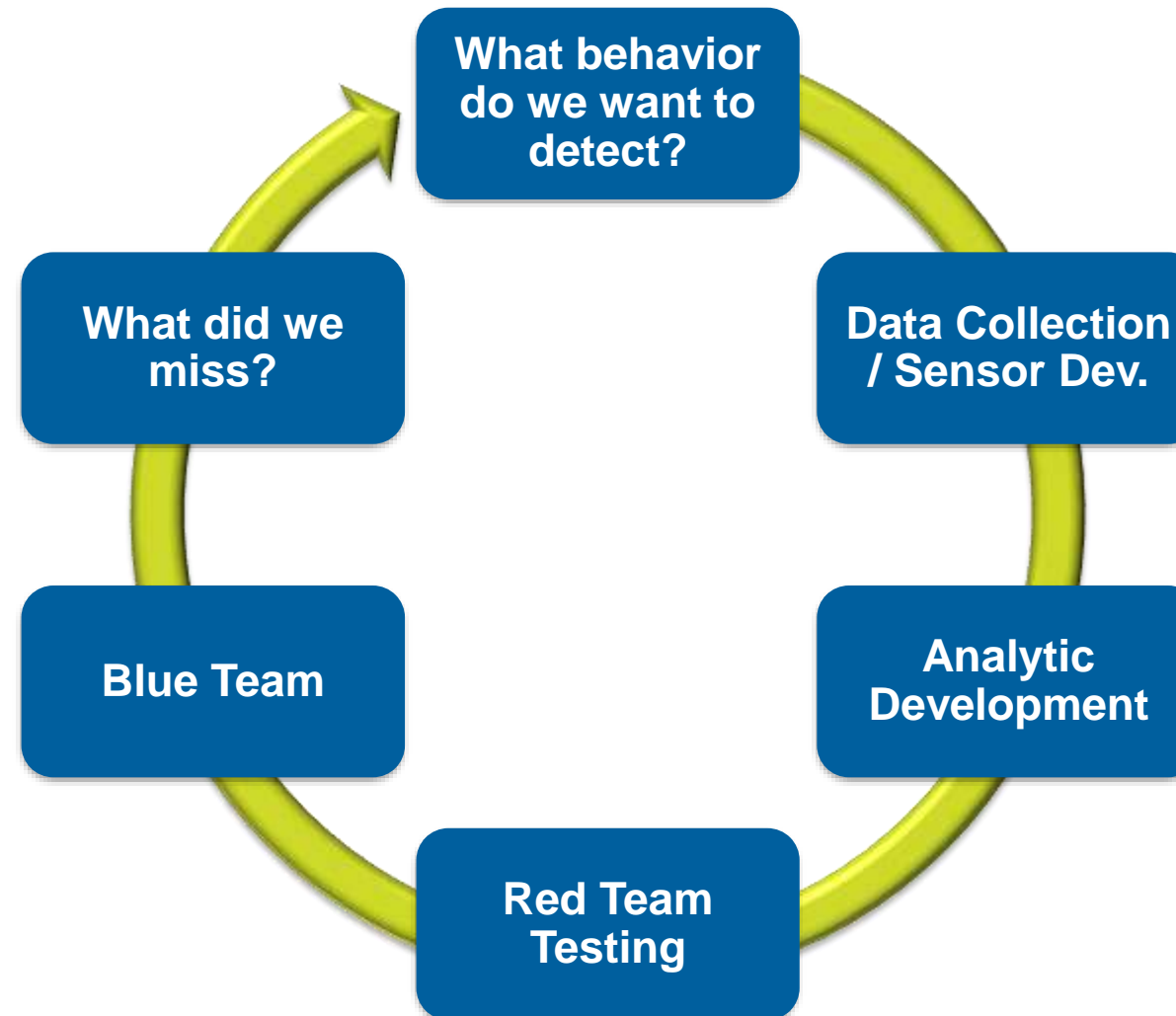
MITRE's Annapolis Junction, MD site

About 250 unclassified computers

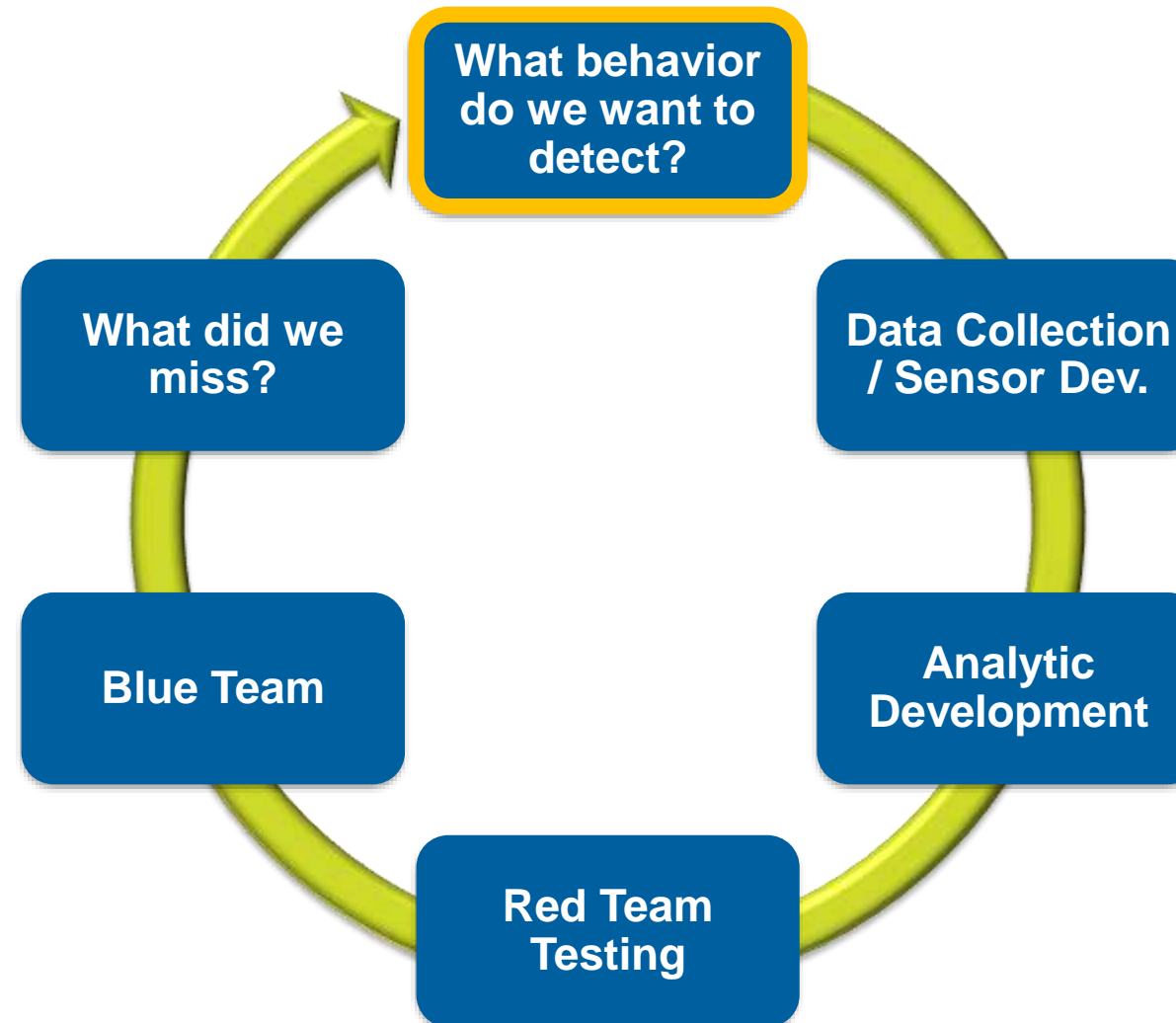
Primarily user desktops running Windows 7



Iterative Analytic Development Cycle

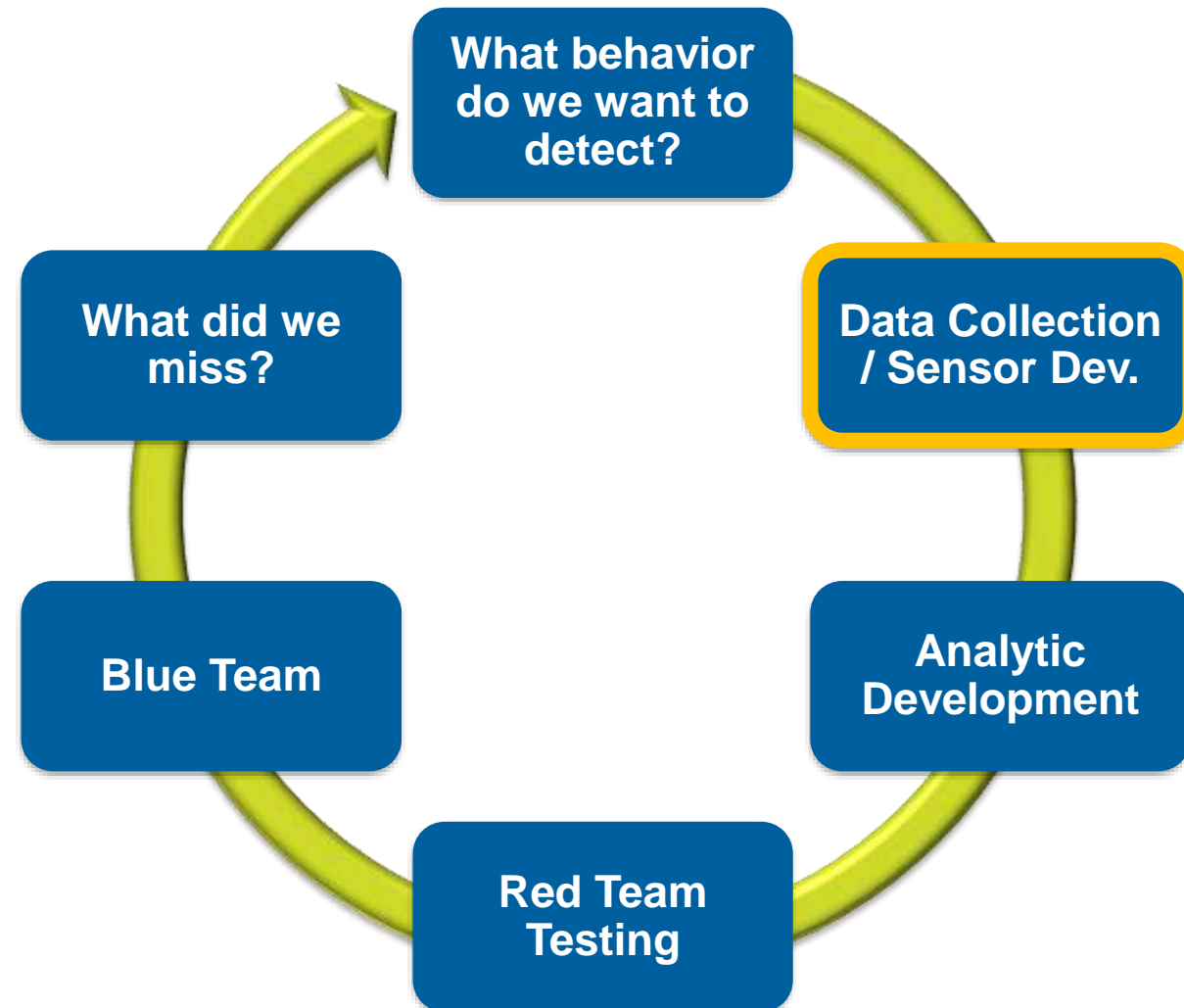


Iterative Analytic Development Cycle



Sensors and Security Tools

Analytic Development Cycle



End-Point Sensing

Addressing the ATT&CK TTPs requires host-level sensing beyond typical antivirus and host-based intrusion sensors

Many more opportunities to catch adversaries operating inside networks than at the perimeter

Better awareness of compromise severity and scope

- Verizon: 85% of IP thefts lacked specific knowledge of what was taken

2013 Verizon Data Breach Investigations Report

Sensor Options

- **COTS**

- CarbonBlack, Mandiant, CrowdStrike, Cylance, others

- **Built-in and OS Integrated**

- Event Tracing for Windows, Sysmon, Autoruns, Event Logs

Sensors: FY16

■ Host-based Sensors

- Microsoft Sysinternals Sysmon
- Custom Event Tracing for Windows Sensor
- Hostflows
- Windows Event Logs
- Microsoft Sysinternals Autoruns
- Splunk Universal Forwarder
 - For facilitation of retrieving logs
 - WinRegMon
 - Stream (testing)

■ Network Sensors

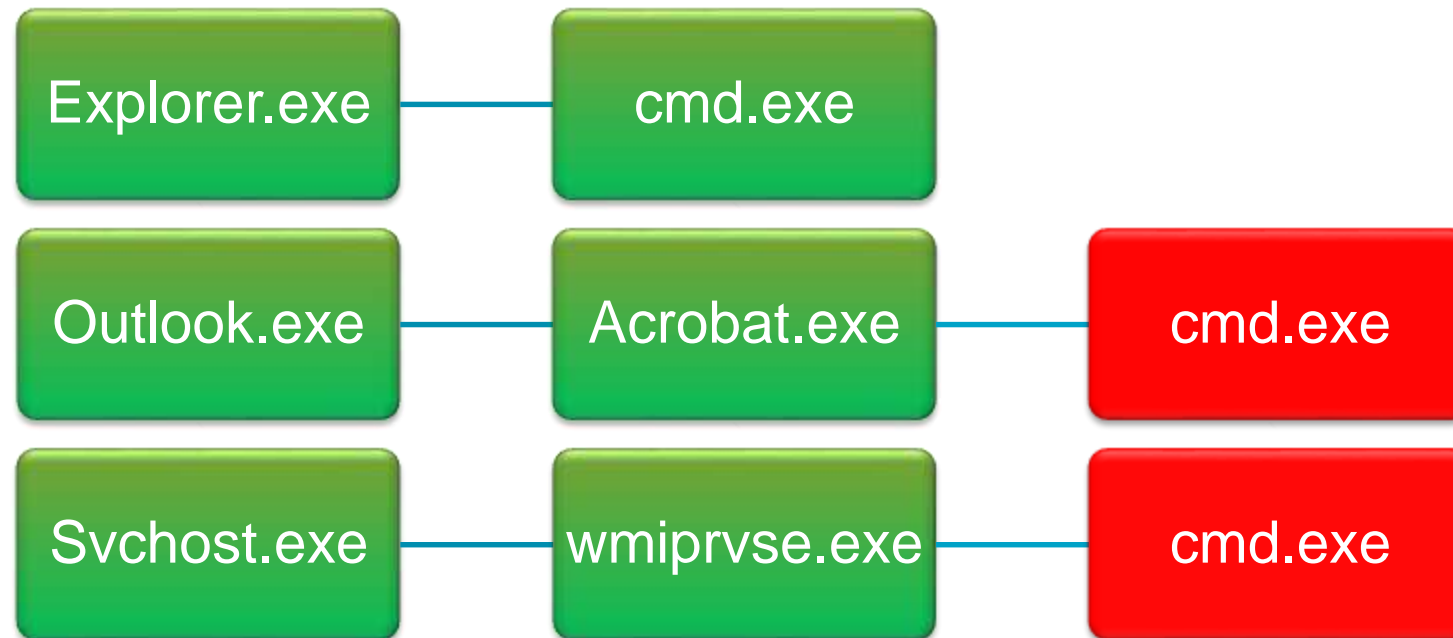
- PCAP
- Netflows
- Suricata



Process Chaining

**Provides details
on processes**

**Process chains provide context
around system activity**



Host Based Network Data

Metadata on network connections

- IP Addresses
- Ports
- Protocol Information
- Message Contents

Pivot point between host and network data

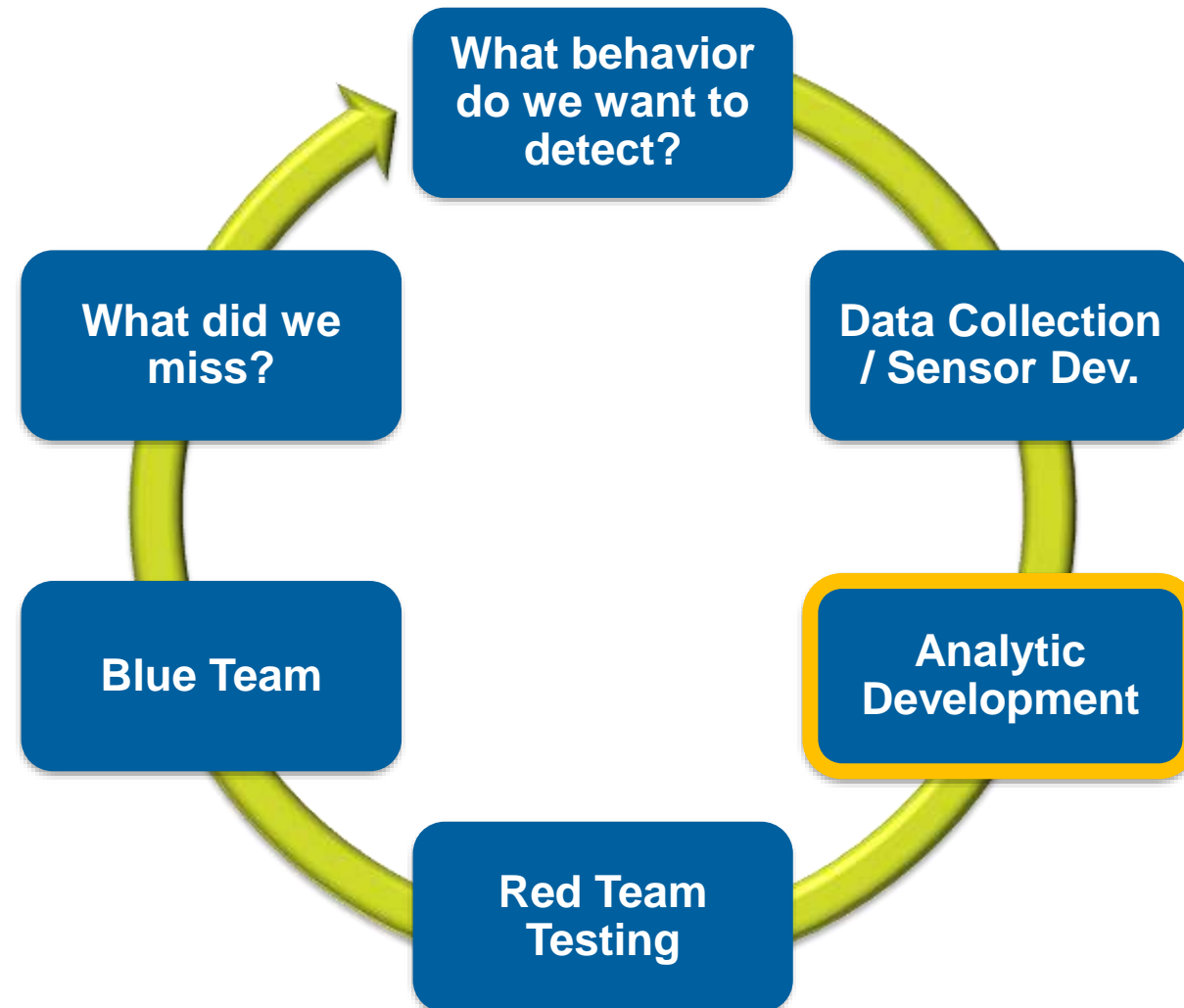
- Process initiating Connection
- PID, PPID

Profile process behavior
Identify covert channels



Analytic Development

Iterative Analytic Development Cycle



Analytic Development

Types of Analytics

Some Types of Analytics

- **TTP Analytics**
- **Situational Awareness**
- **Anomaly/Statistical**
- **Forensic**

TTP Analytics

- Designed to detect a certain adversary tactic, technique or procedure.
- Examples:
 - Suspicious Commands (net.exe, at.exe, etc.)
 - Remotely Launched Services
 - SMB Copy and Execute
 - Services launching cmd.exe
 - SPL:

```
eventtype=process_start image_path=*\cmd.exe  
parent_image_path="*\windows\system32\services.exe"  
| table _time host_name user ppid pid image_path command_line
```

Situational Awareness Analytics

- Analytics geared towards a general understanding of what is occurring within your environment at a given time. Information like login times or running processes don't indicate malicious activity, but when coupled with other indicators can provide much needed additional information.
- Example:
 - Running processes (e.g. security software)
 - Local User Login
 - Psedudocode:
EventCode == 4624 and [target_user_name] != "ANONYMOUS LOGON" AND
[authentication_package_name] == "NTLM"

Anomaly/Statistical Analytics

- **Detection of behavior that is not malicious but unusual and may be suspect. Like Situational Awareness analytics, these types of analytics don't necessarily indicate an attack.**
- **Examples:**
 - **New Executables**
 - **Outlier Parents of cmd.exe**
 - **Clearing Event Logs**
 - **SPL:**
`(eventtype = wineventlog_security EventID=104) OR (eventtype = wineventlog_system AND (EventID=1100 OR EventID=1102))`

Forensic Analytics

- **These types of analytics are most useful when conducting an investigation regarding an event. Oftentimes forensic analytics will need some kind of input to be most useful.**
- **Examples:**
 - **Determine Accounts Compromised by Credential Dumper**
 - **Remote logons to or from the box within a timespan**

Analytic Development

Cyber Analytic Repository

Information for Each Analytic

- **Description**
 - **Description of the hypothesis being tested in the analytic**
 - **Relevant information about the interest or benefit of the alert**
- **Categorical Information**
 - **CAR analytic number:** for alerting and tracking purposes
 - **Submission date**
 - **Information domain:** host v. network
 - **Available and applicable subtypes**
 - **Type of analytic**
 - **Status:** conceptual, active, deprecated, etc.

Information for Each Analytic

- **ATT&CK Detection**

- Summary of the tactic(s) and technique(s) covered by the analytic
- Level of coverage

- **Pseudocode**

- The analytic instantiation defined using pseudocode

- **Unit Tests**

- Requirements, configuration, description, and command applicable to the analytic

Public website – car.mitre.org



Analytic Development

Implementation

Data Model Abstraction

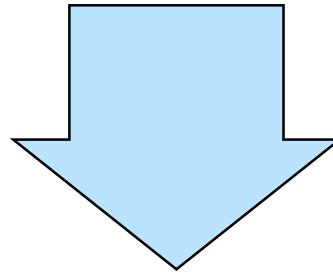
index=old_sensor type=**PROC_EVENT_CREATE** hostname=A4123456.mitre.org imagepath="c:\\location\\foo.exe"

- OR -

index=sysmon Message="**Process Create**" ComputerName=A4123456.mitre.org Image="c:\\location\\foo.exe"

- OR -

index=mcafee sourcetype=hips alert="**process launch**" node_name=A4123456.mitre.org
image_path="c:\\location\\foo.exe"



eventtype=**process_start** host_name=A4123456 image_path="c:\\location\\foo.exe"

Current eventtypes: file_access, process_start, process_stop, flow, logon

Data Model

props.conf in our custom Sysmon TA:

```
[source::WinEventLog:Microsoft-Windows-Sysmon/Operational]
FIELDALIAS-image_path = Image AS image_path
FIELDALIAS-host_name = ComputerName AS host_name
...
EVAL-exe = replace(image_path, ".*\\", "")
EVAL-parent_exe = replace(parent_image_path, ".*\\", "")
...
```

eventtypes.conf in our custom Sysmon TA:

```
[process_start]
search = source=WinEventLog:Microsoft-Windows-Sysmon/Operational EventCode=1
```

■ process_start elements:

- command_line
- exe
- fqdn
- host_name
- image_path
- parent_exe
- parent_image_path
- pid
- ppid
- sid
- user
- uuid

CAR Instantiation with Data Model

CAR-2014-07-001: Search Path Interception

Hypothesis:

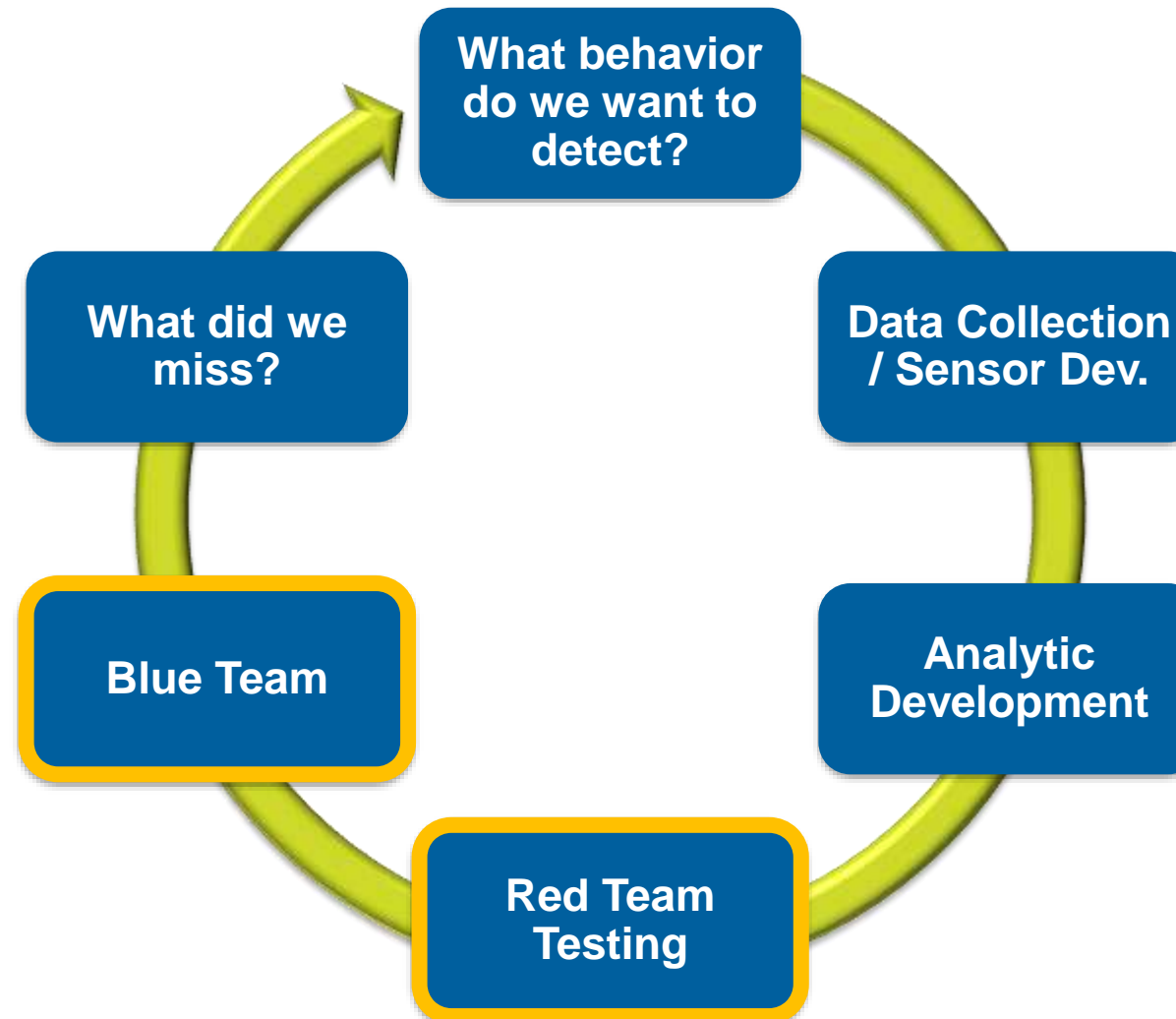
As described by ATT&CK, one method of escalation is intercepting the search path for services, so that legitimate services point to the binary inserted at an intercepted location. This can be done when there are spaces in the path and it is unquoted.

Instantiation:

```
eventtype=process_start parent_image_path="*\\system32\\services.exe" command_line!="*" command_line="* *"
| rex field=image_path ".*\\(?:<img_exe>\\.*)"
| rex field=img_exe "(?<img_base>\\.\\.*)"
| where NOT like(lower(command_line), lower("%"+img_exe+"%")) AND like(lower(command_line), lower("%"+img_base+"%"))
| table _time host_name ppid pid parent_image_path image_path command_line img_exe
```

Evaluating Analytics

Iterative Analytic Development Cycle

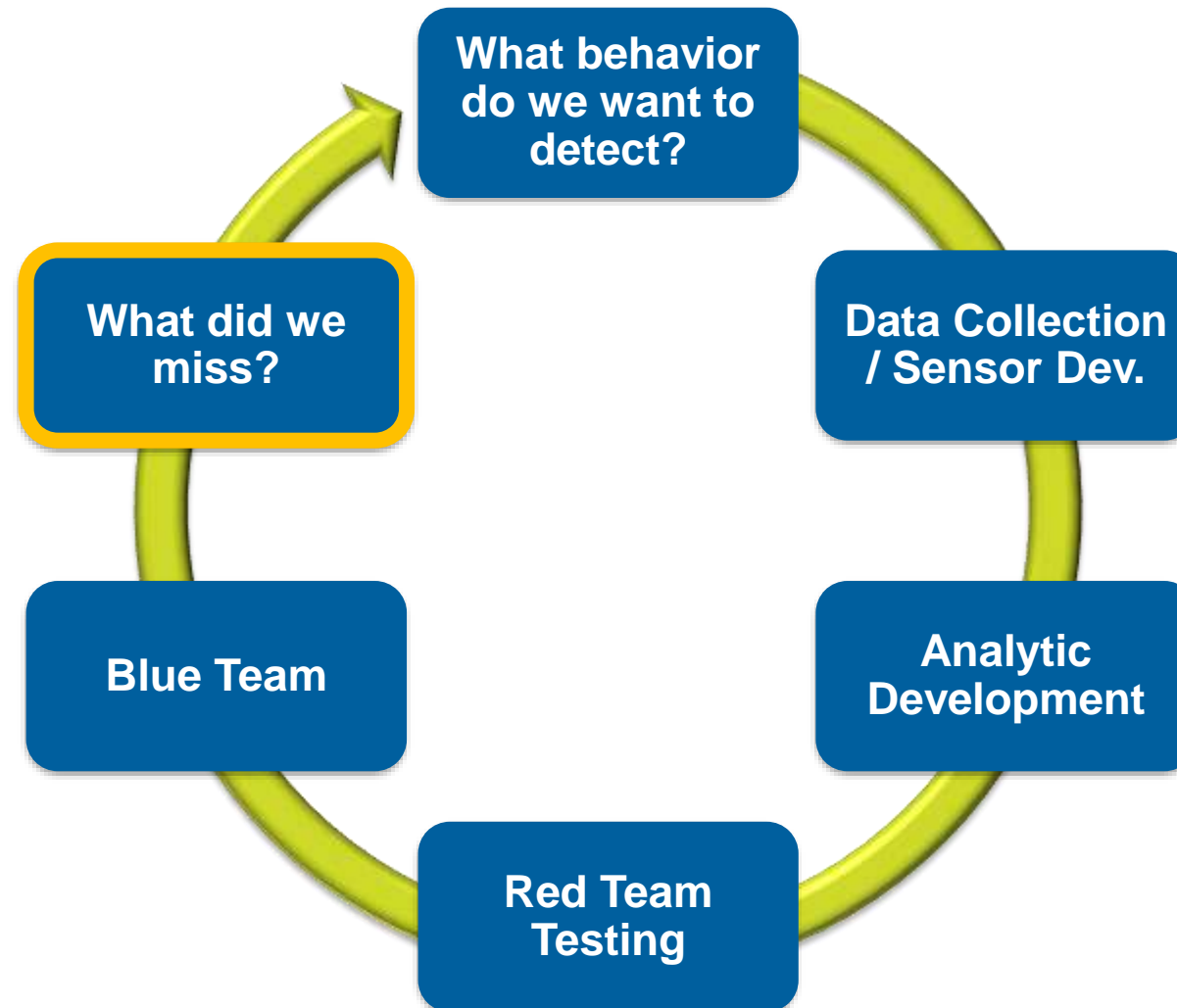


Evaluation with Cyber Games

- **Red/Blue Team operations within production environment**
 - Emulated adversary
 - Asynchronous
 - Designed to push analytic boundaries
- **Goals**
 - What dates did activity occur?
 - What hosts were affected?
 - What credentials were compromised?
 - What was the RT's goal?
 - Was the RT successful?

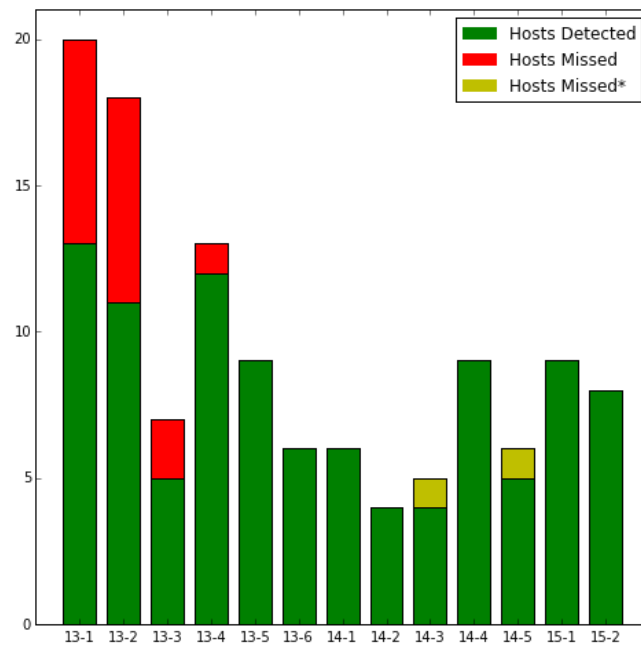


Iterative Analytic Development Cycle

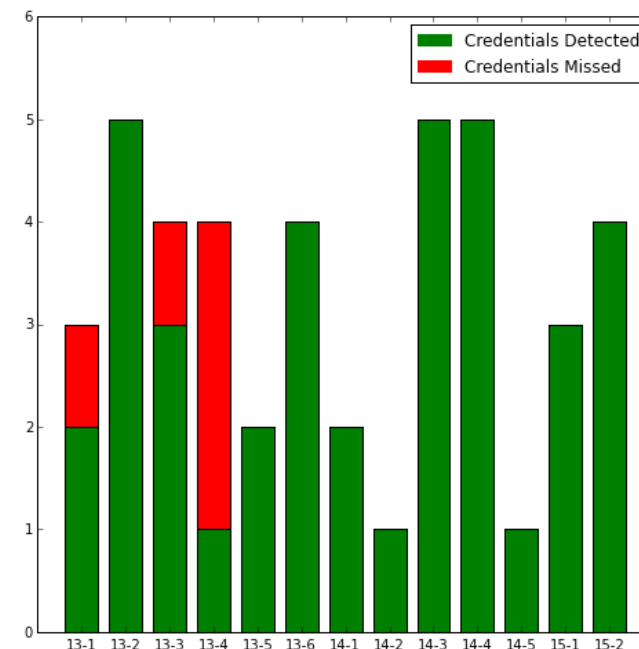


Cyber Game Results

- 13 Cyber Games from 2013-2015
- Detected Significant RT Activity Every Cyber Game



Hosts



Credentials

Summary and Example

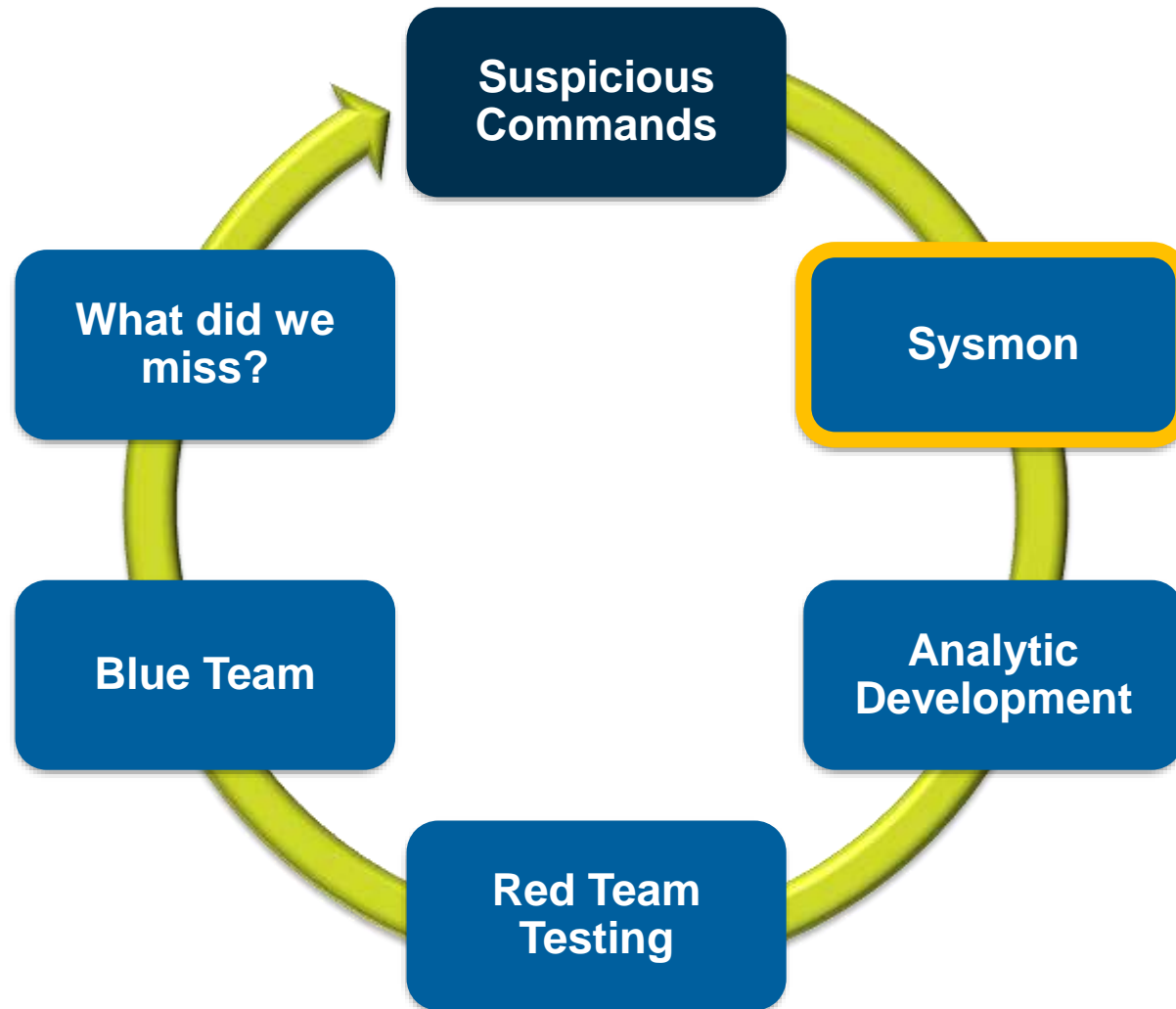
Analytic Development Example



- Certain commands are *frequently used by malicious actors* and *infrequently used by normal users*.
- By looking for execution of these commands in short periods of time, we can not only see when a malicious user was on the system but also get an idea of what they were doing.
- ATT&CK Coverage:

Credential Access	Exfiltration
Defense Evasion	Lateral Movement
Discovery	Persistence
Execution	Privilege Escalation

Do we have the data we need?

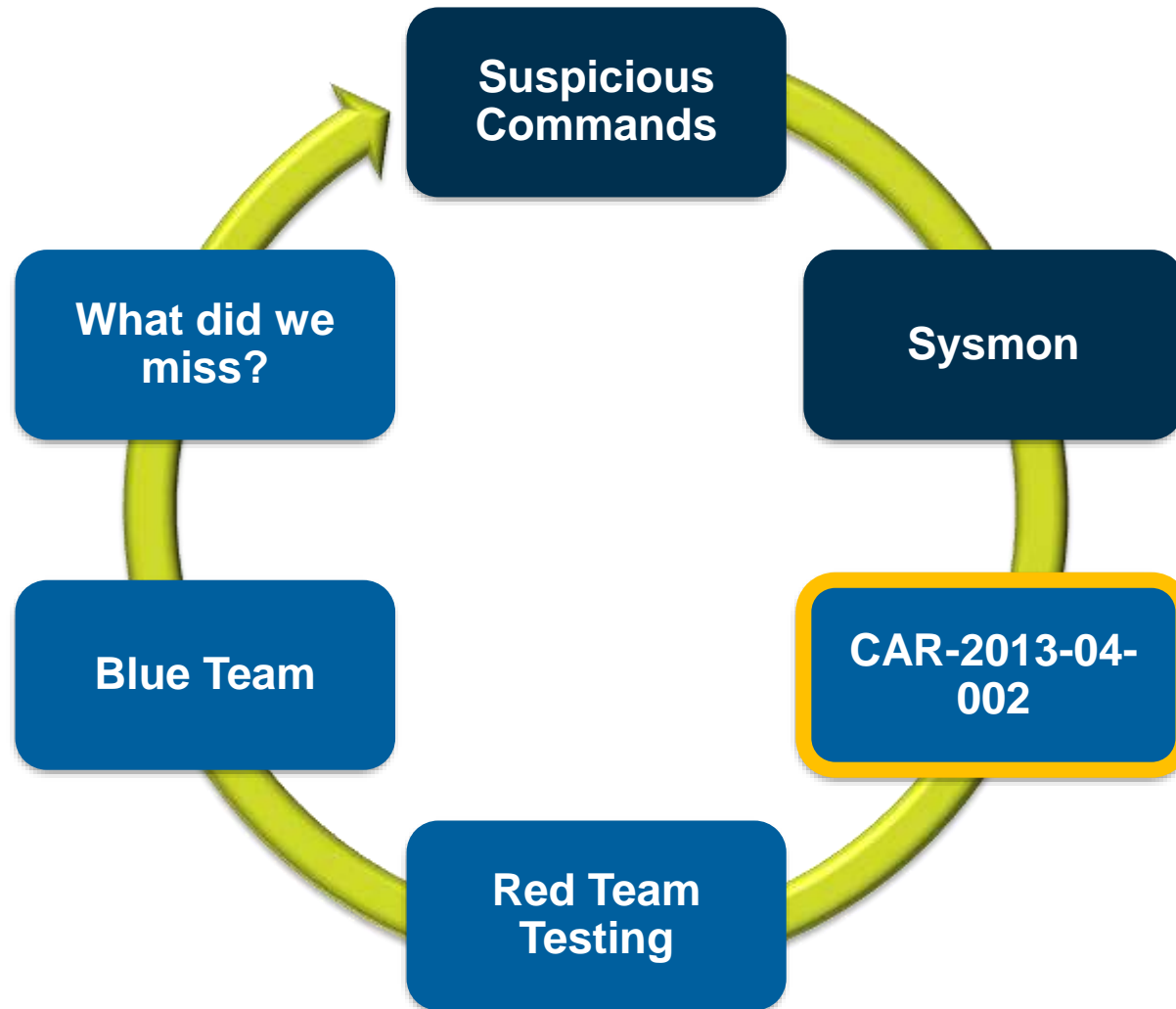


■ Sysmon event example:

```

<Event
  xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon'
  ....<Computer>1234ABCD.DOMAIN.COM</Computer>
  >...</System><EventData><Data
    Name='UtcTime'>2016-08-05
    16:01:13.851</Data>...<Data
    Name='ProcessId'>22520</Data><Data
    Name='Image'>C:\Windows\System32\net.exe</Data>
    <Data Name='CommandLine'>net start
    splunkforwarder</Data>...<Data
    Name='User'>DOMAIN\USER123</Data>...<Data
    Name='ParentProcessId'>10972</Data><Data
    Name='ParentImage'>C:\Windows\System32\cmd.exe
    </Data><Data Name='ParentCommandLine'>cmd /c
    net start splunkforwarder
    </Data></EventData></Event>
  
```

Write the analytic, perform unit tests



```

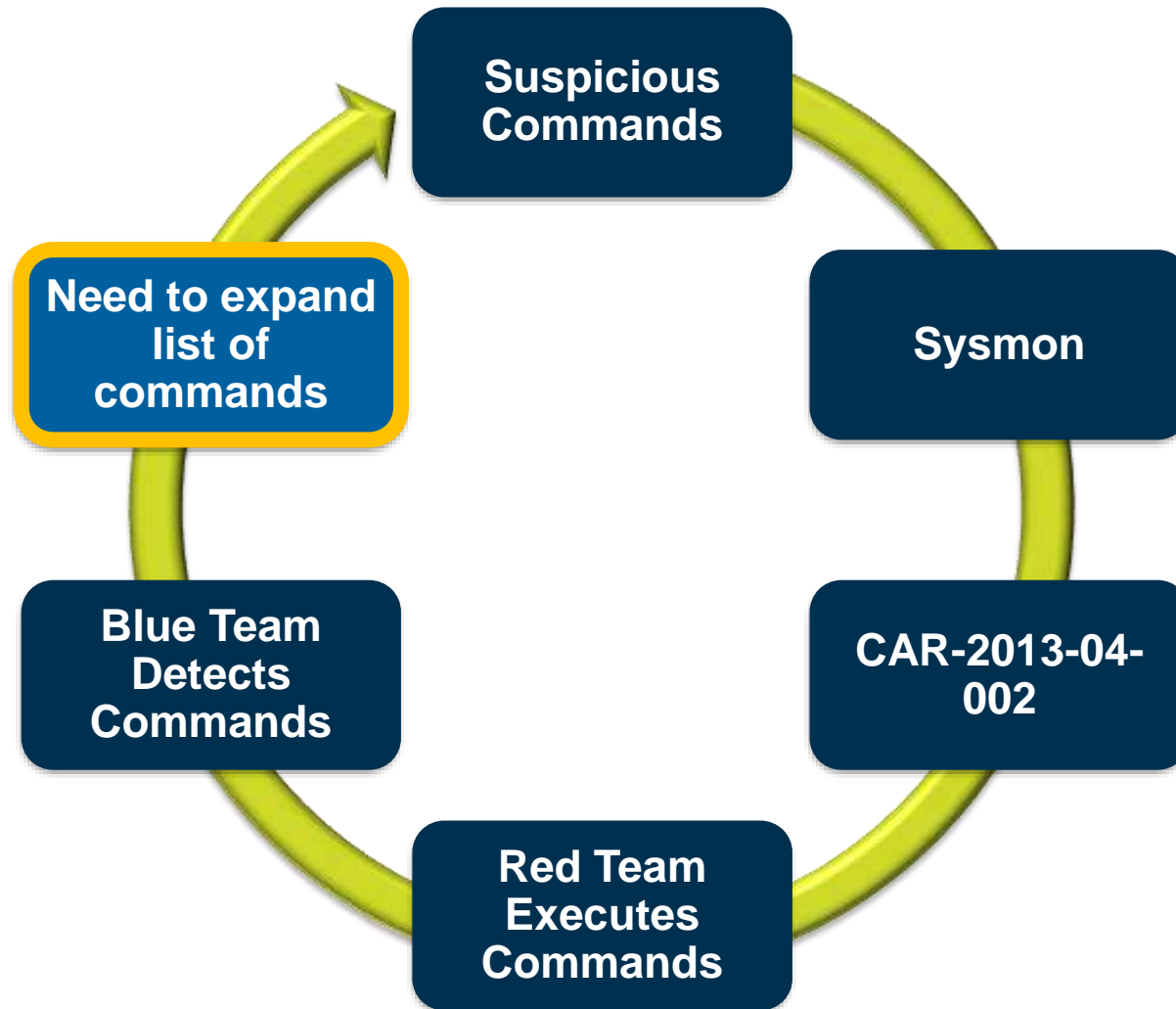
eventtype=process_start exe="arp.exe" OR
exe="at.exe" OR exe="attrib.exe" OR
exe="cscript.exe" OR exe="dsquery.exe"
OR exe="hostname.exe" OR
exe="ipconfig.exe" OR exe="nbstat.exe"
OR exe="net.exe" OR exe="netsh.exe" OR
exe="nslookup.exe" OR exe="mimikatz.exe"
OR exe="ping.exe" OR exe="quser.exe" OR
exe="qwinsta.exe" OR exe="reg.exe" OR
exe="runas.exe" OR exe="sc.exe" OR
exe="ssh.exe" OR exe="systeminfo.exe" OR
exe="taskkill.exe" OR exe="telnet.exe"
OR exe="tracert.exe" OR
exe="wscript.exe"
| stats values(exe) values(UtcTime) by
host ppid parent_exe
  
```


Red Team / Blue Team test



- **Red Team event occurs**
- **Blue team is alerted on the following:**
 - Added service with sc.exe
 - Started service with net.exe
 - Dumped credentials with mimikatz.exe

Hot wash



- **Blue Team missed:**

- Creation of scheduled task via schtasks.exe
- Collection of documents using xcopy.exe

- **Blue Team updates query:**

- Add schtasks.exe
- Add xcopy.exe

Lessons Learned



Our experiments validate that end-point sensing can be used to detect an emulated cyber adversary

Understanding parent / child relationships of processes is highly valuable for identifying malicious behavior

We continue to improve analytics and test sensing capabilities to better detect adversary behavior

Questions?

ATT&CK

attack@mitre.org

Public website:

attack.mitre.org

The Fort Meade Experiment

fmex@mitre.org

Cyber Analytic Repository

car@mitre.org

Public website:

car.mitre.org

Backup

Abstract

Effectively defending a network from Advanced Persistent Threats (APTs) remains a difficult problem for enterprises, as evidenced by the large number of publicly documented network compromises. MITRE has been performing research on ways to detect APTs more quickly post-compromise, once they gain initial access to a network. As part of our research, we developed an adversary model (ATT&CK™), a suite of behavior-based analytics for detecting threats operating on a network, and an iterative method for developing future analytics.

ATT&CK™ is a model and framework for describing the actions an adversary takes while operating within an enterprise network. The model can be used to better characterize post-compromise adversary behavior with the goal of distilling the common behaviors across known intrusion activity into individual actions that an adversary may take to be successful. The techniques described in ATT&CK™ relate to observed APT intrusions, and are at a level of abstraction necessary for effectively prioritizing defensive investments and comparing host-based intrusion detection capabilities.

The ATT&CK Model

■ Consists of:

1. Tactic phases derived from Cyber Attack Lifecycle
2. List of techniques available to adversaries for each phase
3. Possible methods of detection and mitigation
4. Documented adversary use of techniques and software
5. Disambiguation of adversaries

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				Application Window Discovery	Third-party Software		Clipboard Data	Data Compressed	Communication Through Removable Media
Accessibility Features	Binary Packing	Code Signing	Credential Dumping		File and Directory Discovery	Application Deployment Software	Command-line	Data Staged	Data Encrypted
Applet DLLs	Component Firmware			Credential Manipulation			Execution through API	Data from Local System	Data Transfer Size Limits
Local Port Monitor	Component Firmware	DLL Side-Loading	Credentials in Files	Local Network Configuration Discovery	Exploitation of Vulnerability	Graphical User Interface	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
New Service	Path Interception					Local Network Connections Discovery	InstallUI	Data from Removable Media	
Scheduled Task	Disabling Security Tools	File Deletion	Network Sniffing	Local Network Connections Discovery	Logon Scripts	PowerShell	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Service File Permissions Weakness	Scheduled Task	File System Logical Offsets	Two-Factor Authentication Interception	Network Service Scanning	Pass the Hash	Process Hollowing			Exfiltration Over Physical Medium
Service Registry Permissions Weakness	Indicator Blocking			Peripheral Device Discovery	Remote Desktop Protocol	Regsvr32	Input Capture	Exfiltration Over Physical Medium	Multi-Stage Channels
Web Shell	Exploitation of Vulnerability			Permission Group Discovery	Remote File Copy	RunDll32	Screen Capture	Exfiltration Over Physical Medium	Multilayer Communication
Basic Input/Output System	Bypass User Account Control			Process Discovery	Remote Services	Scheduled Task	Scheduled Transfer		
	Bootkit	DLL Injection			Query Registry	Replication Through Removable Media		Scripting	Peer Connections
Change Default File Association	Indicator Removal from Tools	Indicator Removal on Host	Remote System Discovery	Process Discovery	Shared Webroot	Windows Management Instrumentation	Service Execution	Standard Application Layer Protocol	Standard Cryptographic Protocol
Component Firmware				Query Registry	Taint Shared Content				
Hypervisor	InstallUI	Masquerading	Security Software Discovery	System Information Discovery	System Owner/User Discovery	System Service Discovery	Standard Non-Application Layer Protocol	Uncommonly Used Port	Web Service
Logon Scripts									
Modify Existing Service	Masquerading	Modify Registry	System Information Discovery	System Owner/User Discovery	System Service Discovery	System Service Discovery	Standard Non-Application Layer Protocol	Uncommonly Used Port	Web Service
Redundant Access									
Registry Run Keys / Start Folder	Obfuscated Files or Information	Process Hollowing	Redundant Access	Registry/Regmon	Regsvr32	RunDll32	Scripting	Software Packing	Time Synchronization
Security Support Provider									
Shortcut Modification	Process Hollowing	Redundant Access	Registry/Regmon	Regsvr32	RunDll32	Scripting	Software Packing	Time Synchronization	Time Synchronization
Windows Management Instrumentation Event Subscription	Registry/Regmon	Regsvr32	RunDll32	Scripting	Software Packing	Time Synchronization	Time Synchronization	Time Synchronization	Time Synchronization
Winlogon Helper DLL	RunDll32	Scripting	Software Packing	Time Synchronization	Time Synchronization	Time Synchronization	Time Synchronization	Time Synchronization	Time Synchronization

ATT&CK-Based Analytics Development Method

- **Post-compromise detection**
- **Focused on known behaviors**
- **Threat-based model**
- **Iterative by design**
- **Developed in a realistic environment**

About Your Presenter – Michael Kemmerer

■ Work

- Senior Cybersecurity Engineer at The MITRE Corporation
- Principal Investigator of BASIS – Behavioral Analytics for Security: Implementation and Sharing
- EIC - network and endpoint sensor integration and analytic platform engineering

■ Past Presentations

- Detecting the Adversary Post-Compromise with Threat Models and Behavioral Analytics
 - Gartner Security and Risk Management Summit – June 2016
 - US Army Europe G6 Cyber Summit – July 2016
 - Splunk .conf – September 2016
 - The Learning Forum's Cyber Security Risk Council – October 2016
- Discovering threats by monitoring behaviors on endpoints
 - Splunk .conf – October 2014

■ Education

- M.S. in Engineering Management, Cybersecurity focus from UMBC
- B.S. in Electrical Engineering from Lehigh University