HIMSS18 The leading health information and technology conference

WHERE THE WORLD CONNECTS FOR HEALTH

Conference & Exhibition | March 5–9, 2018

Las Vegas | Venetian – Palazzo – Sands Expo Center

Detecting Cyber Threats with ATT&CK™-Based Analytics

Session 123, March 7, 2018

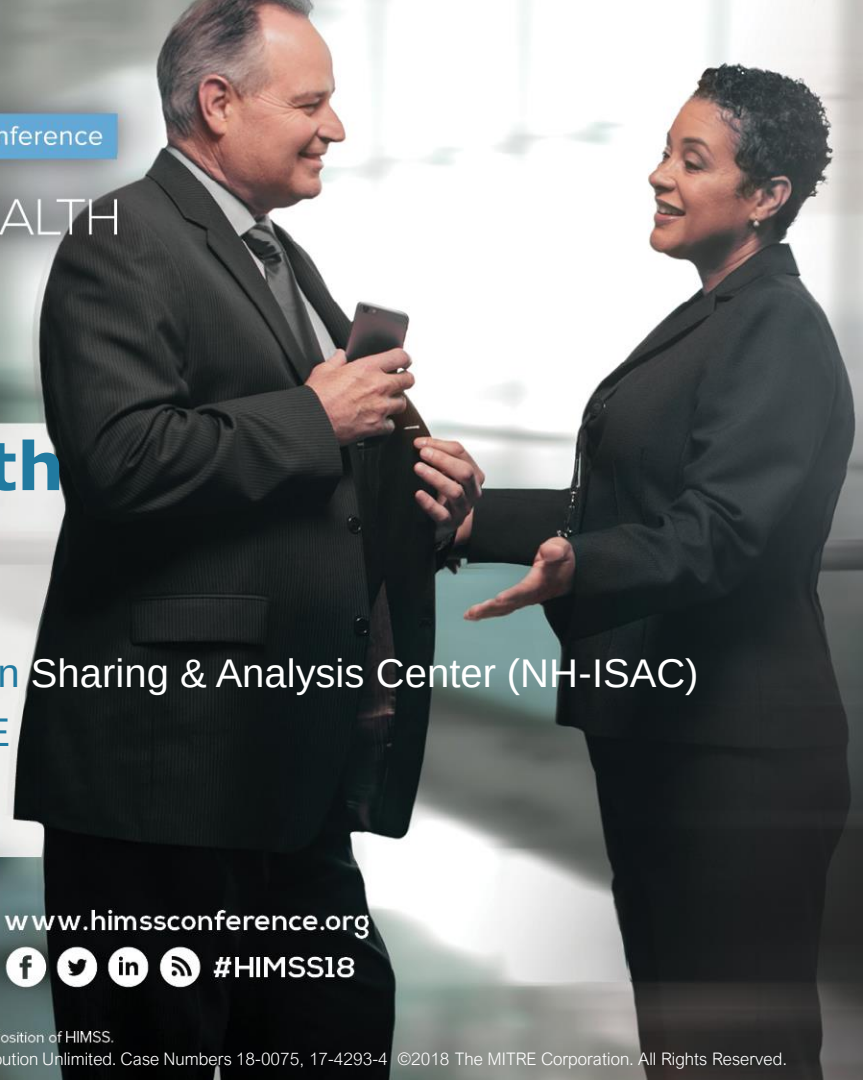
Denise Anderson, President, National Health Information Sharing & Analysis Center (NH-ISAC)

Julie Connolly, Principal Cybersecurity Engineer, MITRE

NH-ISAC NATIONAL HEALTH - ISAC

MITRE

COMMITMENT



www.himssconference.org

#HIMSS18

Conflict of Interest

Denise Anderson, M.B.A.
Julie Connolly, B.S., CISSP

Have no real or apparent conflicts of interest to report.

Agenda

- The Threat Landscape
- Adversarial Tactics, Techniques, & Common Knowledge (ATT&CK™) family of models
- Using ATT&CK™
- Collaborative ATT&CK™ Analytics Development Effort

Learning Objectives

- Explain the Adversarial Tactics, Techniques, & Common Knowledge (ATT&CK™) for Enterprise framework, as well as the broader family of ATT&CK™ models, for characterizing post-compromise adversary behavior
- Describe how to use the ATT&CK™ family of models and the Cyber Analytics Repository (CAR) knowledge base to help identify and mitigate adversary behavior on an enterprise network
- Characterize the collaborative effort for developing ATT&CK™- based analytics to detect post-compromise cyber attackers on healthcare systems and networks

Remember This?

Threat Landscape

Threat Actors

Nation State

Hactivist

Insiders/ Third Party Providers

Media/Vendors

Terrorists

Criminal

Motivation

- Advantage: IP Theft, Infiltration – create future vulnerabilities, Data Theft, Political Blackmail;
- Ego: Prowess, Revenge, Notoriety;
- Ideology: Religious, Cultural, Social, Political
- Greed: Money/Power

Motivation

Advantage/Greed

Ideology/Ego

Ideology/Ego

Greed

Greed

Ideology/Greed

Vectors

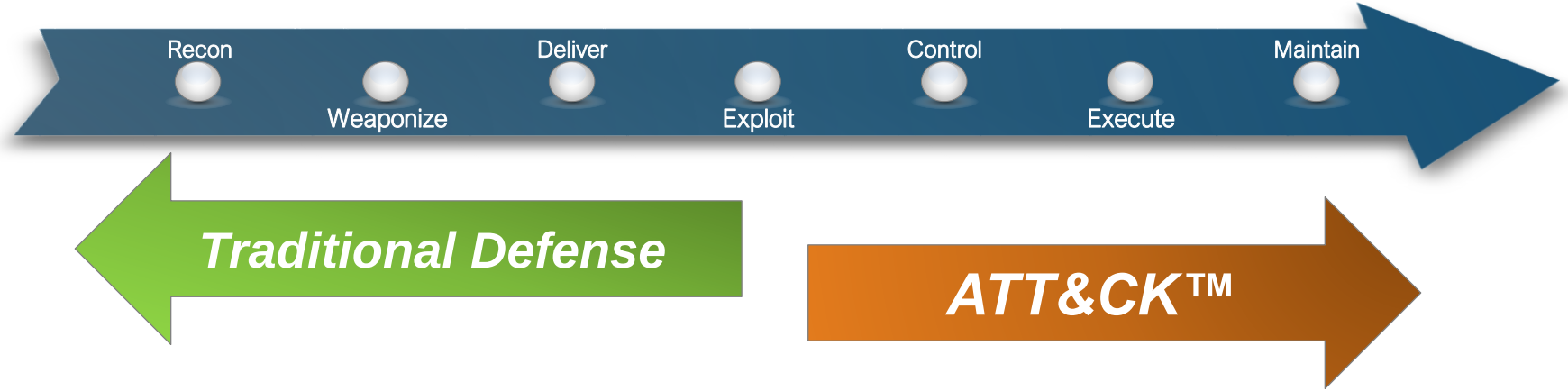
- Botnets: Phishing, Spearphishing
- Viruses, Worms
- Rootkits, Remote Access
- Ransomware
- Wipers
- Trojans
- DDoS

- Vulnerability Scanning, Exploit Kits – Zero Day
- Drive By Downloads, Watering Holes
- Browser exploits
- Point of Sale Malware
- Mobile
- Control Systems

Vectors - Actions

- Remote Access (Infiltration/resource)
- Resource Harvesting (Criminal - Bots)
- Extortion (Criminals)
- Credential Harvesting (Criminals)
- Data Exfiltration (Criminals, Nation State)
- Because it's there (Hacktivist/Terrorist - Defacement, Make Statement, Embarrass)
- Escalate Privilege (Nation State - Infiltration, Criminal)
- Geopolitical Fallout (Nation State – WannaCry, Petya)

The Cyber Attack Lifecycle: Where are we looking?

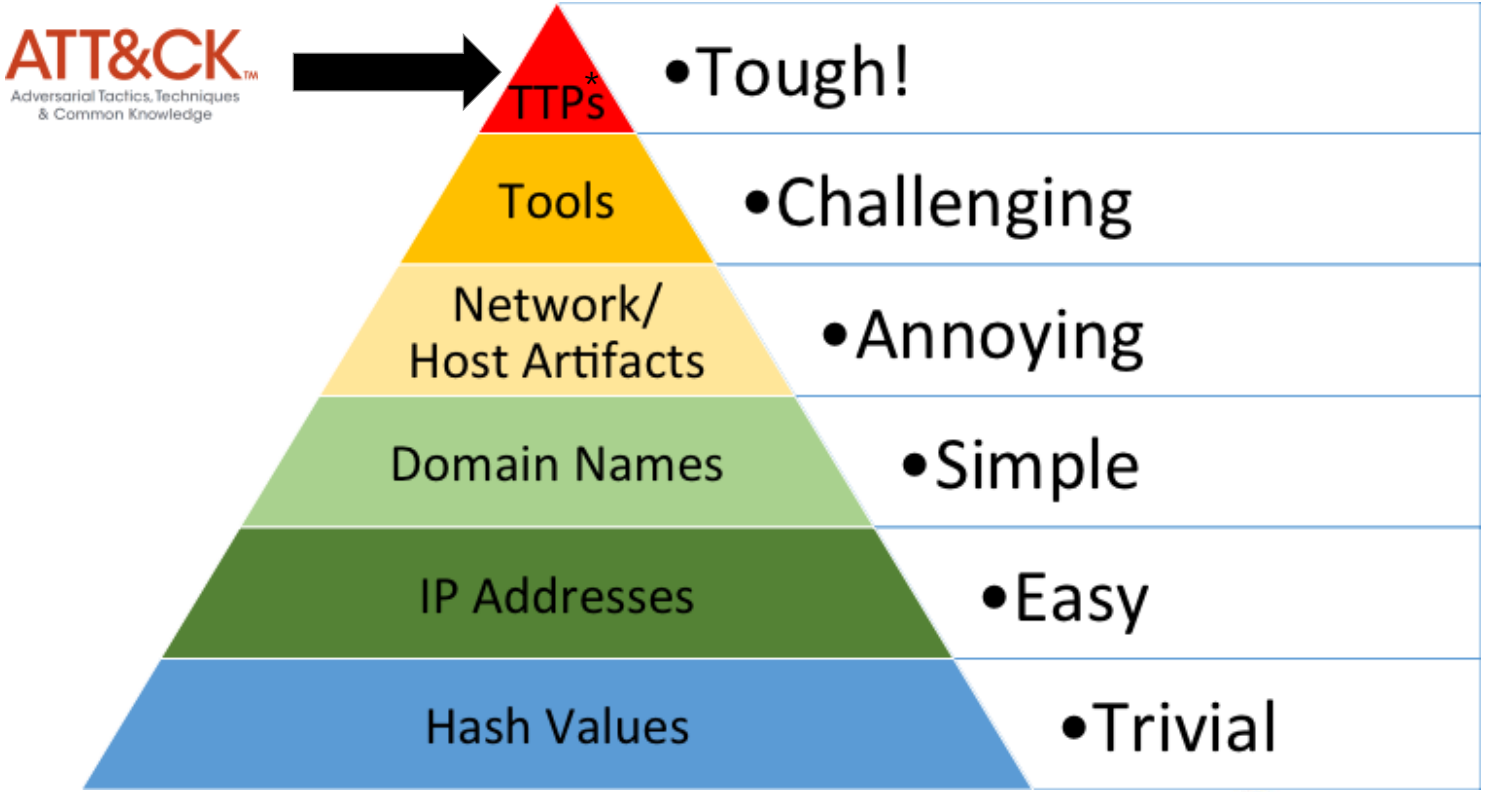


99 days - The median time an adversary is in a network before being detected

-Mandiant, M-Trends 2017

Cyber Attack Lifecycle: The MITRE Corporation https://www.mitre.org/capabilities/cybersecurity/threat-based-defense

Bianco's Pyramid of Pain



*TTPs= Tactics Techniques & Procedures

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

Hard Questions

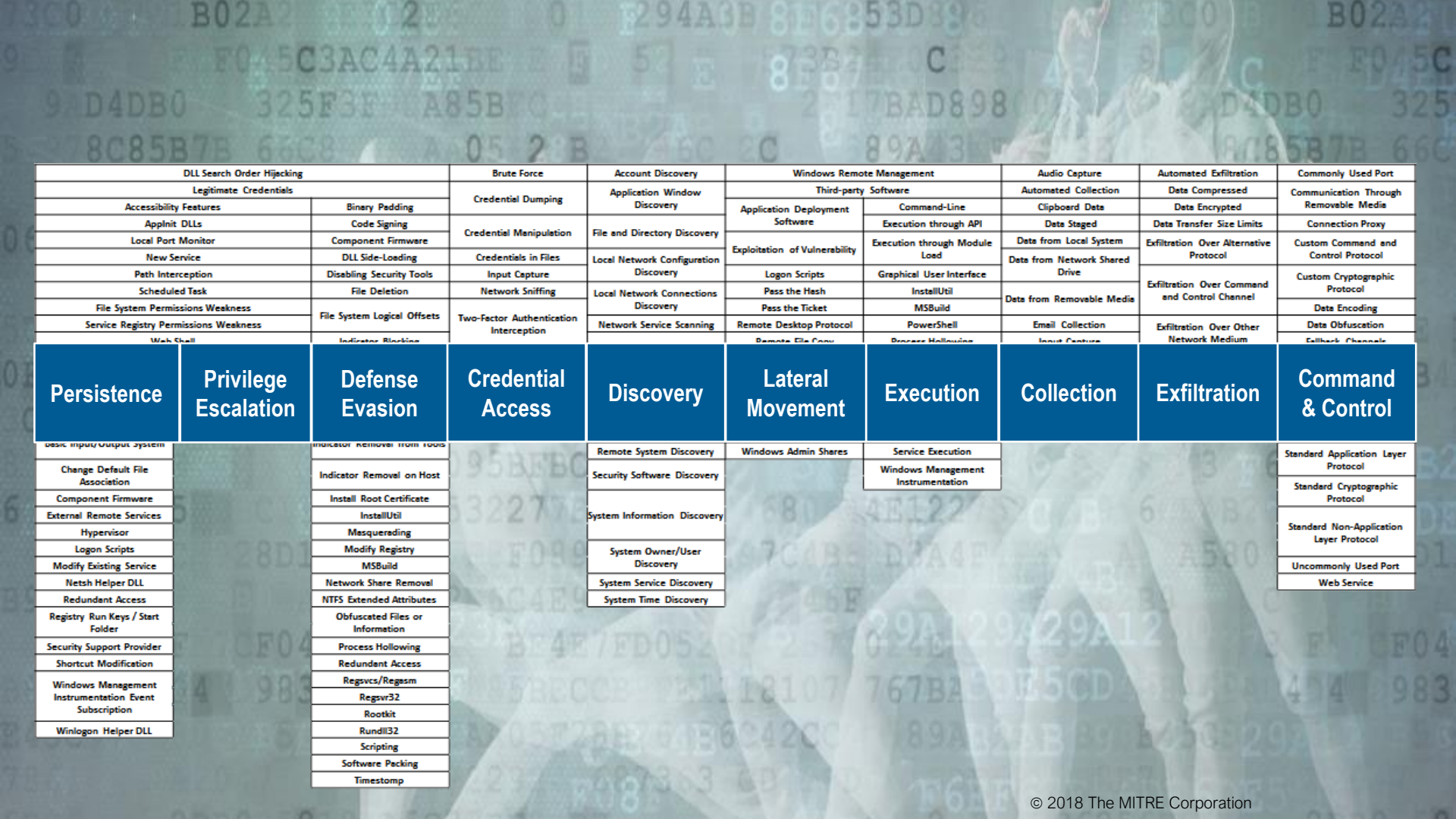
- How do I implement TTP-based detection?
- How effective is my defense?
- What is my detection coverage against APT29?
- Is the data I'm collecting useful?
- Do I have overlapping sensor coverage?
- Is the new product from vendor XYZ of any benefit to my organization?

Adversarial Tactics, Techniques & Common Knowledge (ATT&CK™)

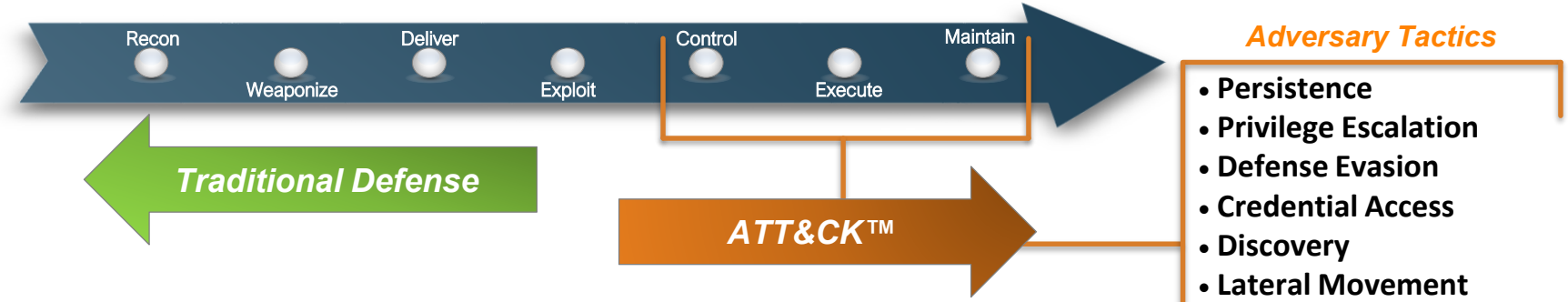
ATT&CK™

ATT&CK™ is a MITRE-developed, globally-accessible knowledge base of adversary tactics and techniques based on real-world observations of adversaries' operations against computer networks.

attack.mitre.org



Breaking Apart the ATT&CK™ Model



What's in ATT&CK?

- ***Tactics*** **– High level, time-agnostic adversary tactical goals**
- ***Techniques*** **– Methods that adversaries use to achieve tactical goals**
- ***Groups*** **– Threat actors, including techniques and software they use**
- ***Software*** **– Built-in utilities and custom malware, linked to techniques**

Full framework at attack.mitre.org

The ATT&CK™ Model

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		Audio Capture	Automated Exfiltration	Commonly Used Port
Legitimate Credentials			Credential Dumping	Application Window Discovery	Third-party Software		Automated Collection	Data Compressed	Communication Through Removable Media
Accessibility Features		Binary Padding			Application Deployment Software	Command-Line	Clipboard Data	Data Encrypted	
AppInit DLLs		Code Signing	Credential Manipulation	File and Directory Discovery		Execution through API	Data Staged	Data Transfer Size Limits	Connection Proxy
Local Port Monitor		Component Firmware			Exploitation of Vulnerability	Execution through Module Load	Data from Local System	Exfiltration Over Alternative Protocol	Custom Command and Control Protocol
New Service		DLL Side-Loading	Credentials in Files	Local Network Configuration			Data from Network Shared		
Path Interception		Disabling Security Tools	Input Capture	Local Netw					
Scheduled Task		File Deletion	Network Sniffing						
File System Permissions Weakness		File System Logical Offsets	Two-Factor Authentication Interception	Networ					
Service Registry Permissions Weakness									
Web Shell		Indicator Blocking		Peripheral De					
Authentication Package	Exploitation of Vulnerability								
	Bypass User Account Control			Permission Groups Discov	Replication Through	Regsvr32	Video Capture	Medium	Multiband Communication
Bootkit	DLL Injection								
Component Object Model Hijacking		Component Object Model Hijacking		Proces					
Basic Input/Output System		Indicator Removal from Tools							
Change Default File Association		Indicator Removal on Host		Remote S					
Component Firmware		Install Root Certificate		Security Softwa		Instrumentation			Standard Cryptographic Protocol
External Remote Services		InstallUtil							
Hypervisor		Masquerading		System Inf Di					
Logon Scripts		Modify Registry		Sys					
Modify Existing Service		MSBuild							
Netsh Helper DLL		Network Share Removal		System Servi					
Redundant Access		NTFS Extended Attributes		System Time 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							
		Timestomp							

Grounded in real data from cyber incidents

Enables pivoting between red team and blue team

Decouples the problem from the solution

Transforms thinking by focusing on post-exploit adversary behavior

#HIMSS18

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

Persistence: New Service example (Continued)

Mitigation:

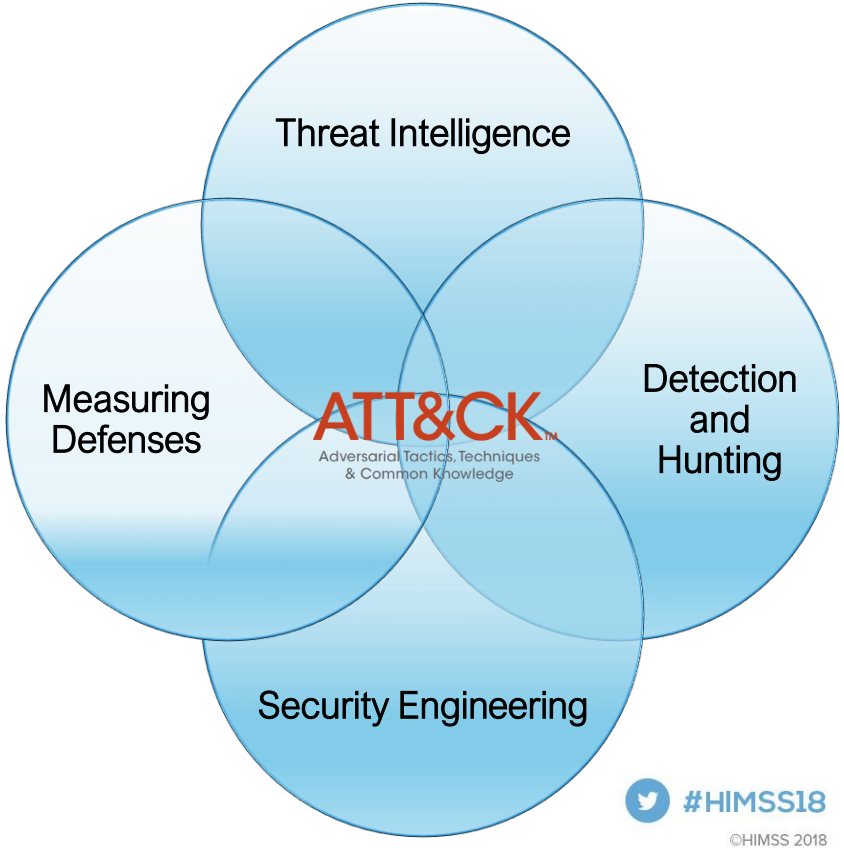
Limit privileges of user accounts and remediate Privilege Escalation vectors
Identify and block unnecessary system utilities or potentially malicious software that may be used to create services

Data Sources: Windows Registry, process monitoring, command-line parameters

Examples: *Carbanak*, *Lazarus Group*, TinyZBot, Duqu, CozyCar, CosmicDuke, hcdLoader, …

ATT&CK™ Use Cases

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



Threat Intel: What do you need to worry about? (NOTIONAL)

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

White-shaded cells have no usage; darker cells have more.

Based on threat intelligence (internal, government-source, open-source).

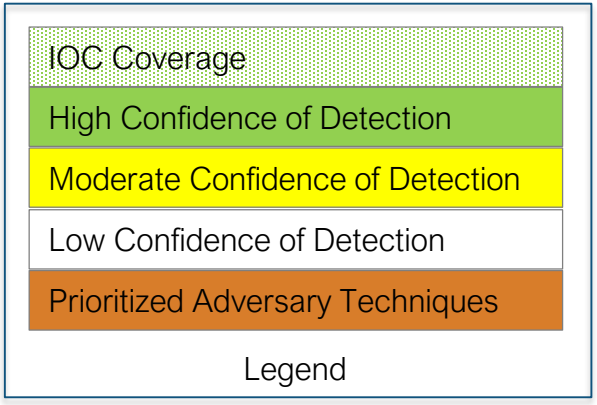
Measuring Defense: What can you cover? (NOTIONAL)

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
DLL Search Order Hijacking			Brute Force	Account Discovery	Windows Remote Management		Automated Collection	Automated Exfiltration	Commonly Used Port
Legitimate Credentials			Credential Dumping	Application Window Discovery	Third-party Software		Clipboard Data	Data Compressed	Communication Through Removable Media
Accessibility Features		Binary Padding			Application Deployment Software	Command-Line	Data Staged	Data Encrypted	
AppInit DLLs		Code Signing	Credential Manipulation	File and Directory Discovery		Execution through API	Data from Local System	Data Transfer Size Limits	Custom Command and Control Protocol
Local Port Monitor		Component Firmware			Exploitation of Vulnerability	Graphical User Interface	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	
New Service		DLL Side-Loading	Credentials in Files	Local Network Configuration Discovery		InstallUtil			Custom Cryptographic Protocol
Path Interception		Disabling Security Tools	Input Capture		Logon Scripts	PowerShell	Data from Removable Media	Exfiltration Over Command and Control Channel	
Scheduled Task		File Deletion	Network Sniffing	Local Network Connections Discovery	Pass the Hash	Process Hollowing			Data Obfuscation
File System Permissions Weakness		File System Logical Offsets	Two-Factor Authentication Interception		Pass the Ticket	Regsvcs/Regasm	Email Collection		Fallback Channels
Service Registry Permissions Weakness				Network Service Scanning	Remote Desktop Protocol	Regsvr32	Input Capture	Exfiltration Over Other Network Medium	Multi-Stage Channels
Web Shell		Indicator Blocking		Peripheral Device Discovery	Remote File Copy	Rundll32	Screen Capture		Multiband Communication
Basic Input/Output System	Exploitation of Vulnerability				Remote Services	Scheduled Task	Audio Capture	Exfiltration Over Physical Medium	
Bootkit	Bypass User Account Control			Permission Groups Discovery	Replication Through Removable Media	Scripting	Video Capture		Multilayer Encryption
Change Default File Association	DLL Injection			Process Discovery	Shared Webroot	Service Execution		Scheduled Transfer	Peer Connections
Component Firmware	Component Object Model Hijacking	Indicator Removal from Tools		Query Registry	Taint Shared Content	Windows Management Instrumentation			Remote File Copy
Hypervisor		Indicator Removal on Host		Remote System Discovery	Windows Admin Shares	MSBuild			Standard Application Layer Protocol
Logon Scripts				Security Software Discovery		Execution through Module Load			Standard Cryptographic Protocol
Modify Existing Service		InstallUtil		System Information Discovery					Standard Non-Application Layer Protocol
Redundant Access		Masquerading		System Owner/User Discovery					Uncommonly Used Port
Registry Run Keys / Start Folder		Modify Registry		System Service Discovery					Web Service
Security Support Provider		NTFS Extended Attributes		System Time Discovery					Data Encoding
Shortcut Modification		Obfuscated Files or Information							
Windows Management Instrumentation Event Subscription		Process Hollowing							
Winlogon Helper DLL		Redundant Access							
Netsh Helper DLL		Regsvcs/Regasm							
Authentication Package		Regsvr32							
External Remote Services		Rootkit							
		Rundll32							
		Scripting							
		Software Packing							
		Timestomp							
		MSBuild							
		Network Share Removal							
		Install Root Certificate							

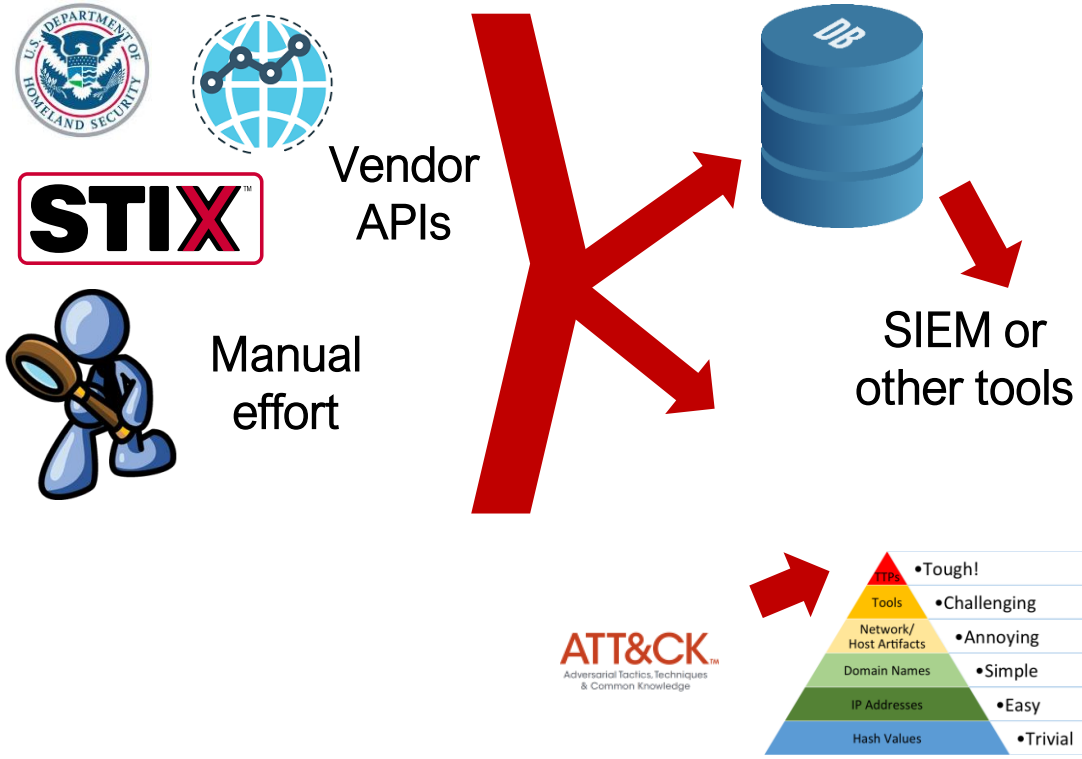
High Confidence	Med Confidence	No Confidence

Prioritized ATT&CK Coverage Matrix (NOTIONAL)

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
DLL Search Order Hijacking			Brute Force	Account Discovery	Windows Remote Management		Automated Collection	Automated Exfiltration	Commonly Used Port
Legitimate Credentials			Credential Dumping	Application Window Discovery	Third-party Software		Clipboard Data	Data Compressed	Communication Through Removable Media
Accessibility Features		Binary Padding			Application Deployment Software	Command-Line	Data Staged	Data Encrypted	
AppInit DLLs		Code Signing	Credential Manipulation	File and Directory Discovery		Execution through API	Data from Local System	Data Transfer Size Limits	Custom Command and Control Protocol
Local Port Monitor		Component Firmware			Exploitation of Vulnerability	Graphical User Interface	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	
New Service		DLL Side-Loading	Credentials in Files	Local Network Configuration Discovery		InstallUtil			Custom Cryptographic Protocol
Path Interception		Disabling Security Tools	Input Capture		Logon Scripts	PowerShell	Data from Removable Media	Exfiltration Over Command and Control Channel	
Scheduled Task		File Deletion	Network Sniffing	Local Network Connections Discovery	Pass the Hash	Process Hollowing			Data Obfuscation
File System Permissions Weakness		File System Logical Offsets	Two-Factor Authentication Interception		Pass the Ticket	Regsvcs/Regasm	Email Collection		Fallback Channels
Service Registry Permissions Weakness				Network Service Scanning	Remote Desktop Protocol	Regsvr32	Input Capture	Exfiltration Over Other Network Medium	Multi-Stage Channels
Web Shell		Indicator Blocking		Peripheral Device Discovery	Remote File Copy	Rundll32	Screen Capture		Multiband Communication
Basic Input/Output System	Exploitation of Vulnerability				Remote Services	Scheduled Task	Audio Capture		
Bootkit	Bypass User Account Control			Permission Groups Discovery	Replication Through Removable Media	Scripting	Video Capture	Exfiltration Over Physical Medium	Multilayer Encryption
Change Default File Association	DLL Injection					Service Execution			Peer Connections
Component Firmware	Component Object Model Hijacking	Indicator Removal from Tools		Process Discovery	Shared Webroot	Windows Management Instrumentation		Scheduled Transfer	Remote File Copy
Hypervisor		Indicator Removal on Host		Query Registry	Taint Shared Content				Standard Application Layer Protocol
Logon Scripts				Remote System Discovery	Windows Admin Shares	MSBuild			Standard Cryptographic Protocol
Modify Existing Service		InstallUtil		Security Software Discovery		Execution through Module Load			
Redundant Access		Masquerading		System Information Discovery					Standard Non-Application Layer Protocol
Registry Run Keys / Start Folder		Modify Registry		System Owner/User Discovery					Uncommonly Used Port
Security Support Provider		NTFS Extended Attributes		System Service Discovery					Web Service
Shortcut Modification		Obfuscated Files or Information		System Time Discovery					Data Encoding
Windows Management Instrumentation Event Subscription		Process Hollowing							
Winlogon Helper DLL		Redundant Access							
Netsh Helper DLL		Regsvcs/Regasm							
Authentication Package		Regsvr32							
External Remote Services		Rootkit							
		Rundll32							
		Scripting							
		Software Packing							
		Timestomp							
		MSBuild							
		Network Share Removal							
		Install Root Certificate							



Using ATT&CK™ to Improve Threat Intelligence-based Cyber Defense



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

Challenges

- Indicators without context are almost useless
  - Provide context!
- Manual effort makes analysts miserable
  - Automate your feeds!
- Adversaries switch indicators constantly, detecting TTPs is more resilient
  - Add analytic sharing

Sounds great, but how do I do this?

Symantec Official Blog

+6
6 Votes

Sowbug: Cyber espionage group targets South American and Southeast Asian governments

Group uses custom Felismus malware and has a particular interest in South American foreign policy.

Symantec Security Response
View Profile

By: Symantec Security Response SYMANTEC EMPLOYEE

Created 07 Nov 2017 | 0 Comments | : 简体中文 日本語

Data Compressed

Data from Network Shared Drive

They attempted to extract all Word documents stored on a file server belonging to this division by bundling them into a RAR archive by running the following command:

Command-Line Interface

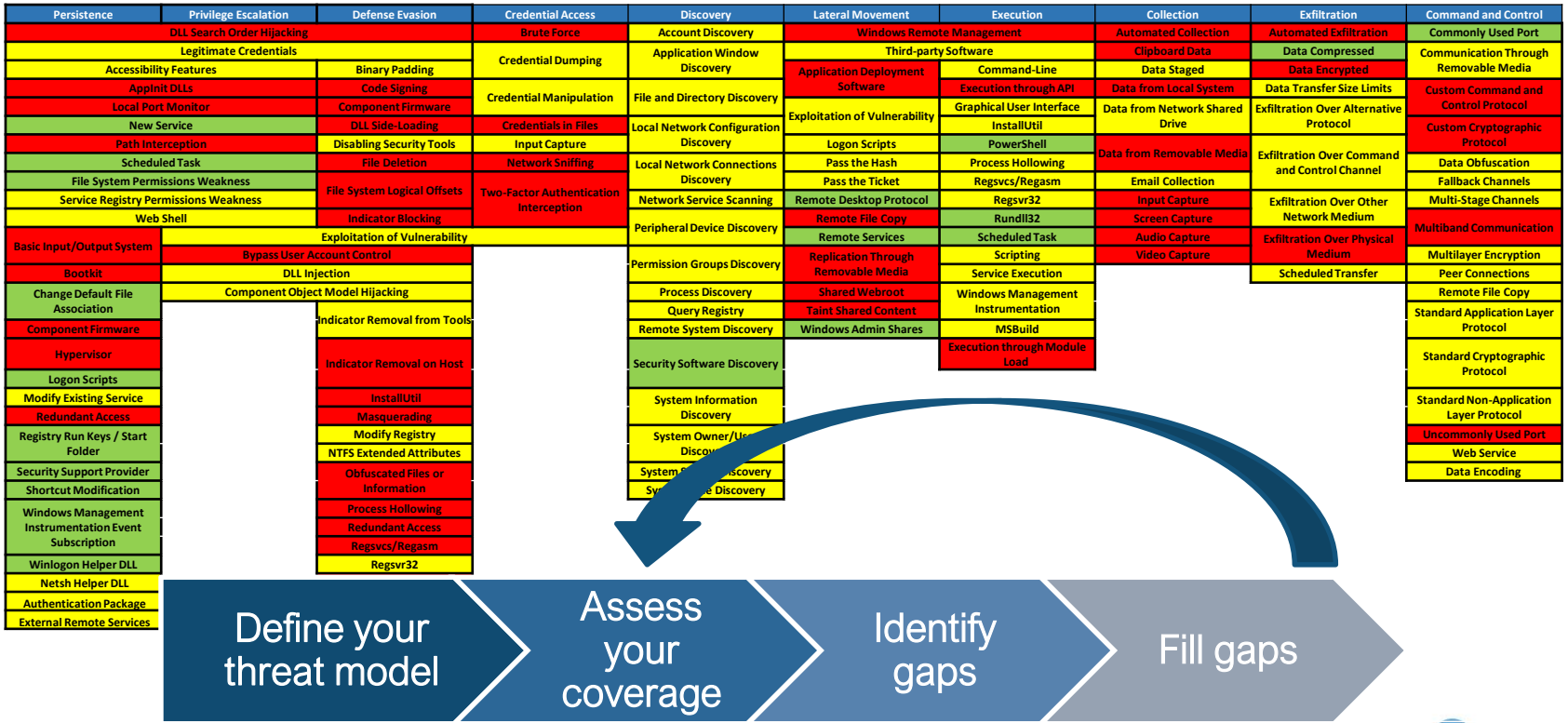
```
cmd.exe /c c:\windows\rar.exe a -m5 -r -ta20150511000000 -v3072 c:\recycler\[REDACTED].rar "\\[REDACTED]\*.docx"
\\[REDACTED]\*.doc.
```

File and Directory Discovery

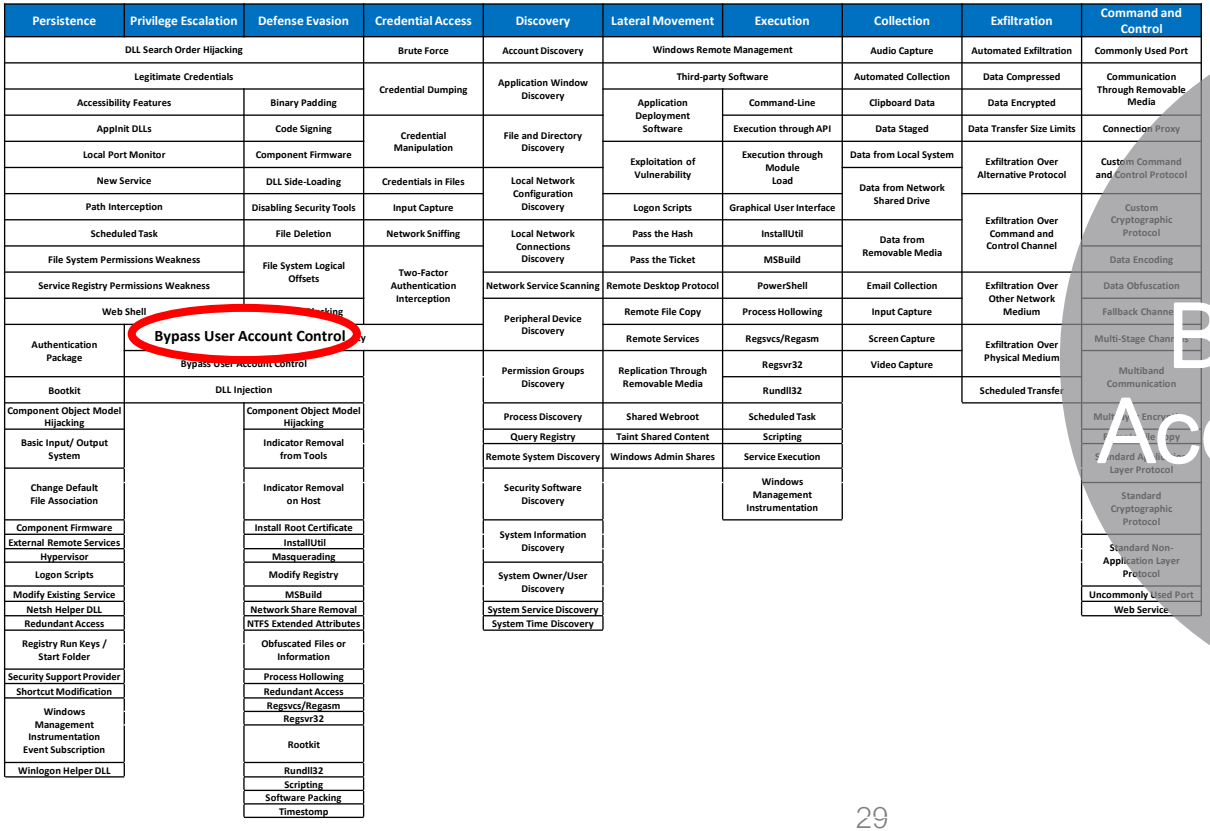
Implementation Tips

- **Tailor your existing threat intel repository**
  - The MISP threat sharing platform has an ATT&CK taxonomy http://www.misp-project.org
  - ATT&CK API
  - ATT&CK in Structured Threat Information eXpression 2.0 (STIX) : https://github.com/mitre/cti
- **Have the threat intel originator do it**
- **Start at the tactic level**
- **Use existing website examples**
- **Choose appropriate information**
- **Work as a team**
- **Remember it's still human analysis**

Look at all those gaps!



Start somewhere



Example: Bypass User Account Control (T1088)

#HIMSS18

Use what you have

- **You probably already have a SIEM platform**
  - Think back: where does ATT&CK focus? Where can we get the most gain?
  - What logs do you already have that can help?
- **Can you collect more? What's the biggest bang for your buck?**
  - Don't turn on everything at once – focus on filling those gaps
- **Read, talk, and work together**

Building an analytic

- **Read the ATT&CK page and understand the attack**
  - Look at references for who's using it and how
  - Think from an adversary perspective
  - Try to mentally separate legitimate usage from malicious usage
- **Try it**
  - Focus on detection
  - Carry out the attacks via your own testing or pre-written scripts
  - What does it look like in the logs?
- **Write and iterate**
  - Write your first search, narrow down false positives, and iterate
  - Keep testing – make sure you check for a variety of ways it can be used, not just the easiest

Filling the gaps is hard, time-consuming, and expensive.

- There are a lot of prevalent techniques
- Adversary practices are always evolving
- Techniques have a wide set of procedures
- We all have limited resources
- Requires in-depth expertise of system internals

Make it a team sport

Tackling the problem **together** is the only way we can keep up

- More brainpower = faster progress
- A broader array of expertise = broader coverage

Multi-faceted approach

- Start out in small working groups
- Not everyone is a producer, feedback is just as important
- Combined with public, open-source, sharing

NH-ISAC Working Group:

Building out and sharing analytics to cover techniques in the ATT&CK™ matrix

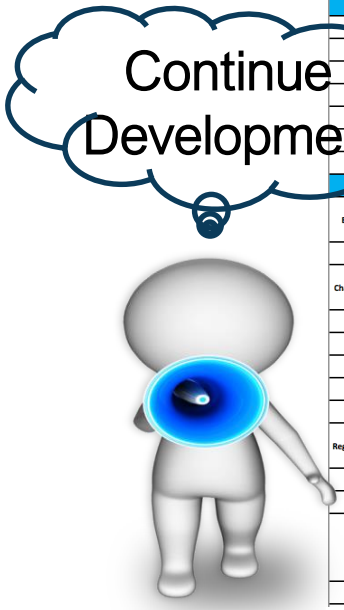
NH-ISAC Analytics Working Group

- **January 2017 kickoff**
- **Mission: Work together to develop analytics to detect ATT&CK techniques**
- **How it works:**
  - Each organization commits to
    - developing analytics and sharing them *or*
    - testing and providing feedback on shared analytics

NH-ISAC Analytics Working Group (Continued)

- **Regular interactions:**
  - Teleconference every 2 weeks to talk about an analytic
  - Annual face-to-face meetings
  - Meet-ups during NH-ISAC summits
- **How it's going:**
  - Shared analytics
  - Shared best practices and tips on how to better collect data required for analytics

NH-ISAC Analytics Working Group Next Steps



Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
DLL Search Order Hijacking			Brute Force	Account Discovery	Windows Remote Management		Automated Collection	Automated Exfiltration	Commonly Used Port
Legitimate Credentials			Credential Dumping	Application Window Discovery	Third-party Software		Clipboard Data	Data Compressed	Communication Through Removable Media
Accessibility Features		Binary Padding			Application Deployment Software	Command-Line	Data Staged	Data Encrypted	
AppInit DLLs		Code Signing	Credential Manipulation	File and Directory Discovery		Execution through API	Data from Local System	Data Transfer Size Limits	Custom Command and Control Protocol
Local Port Monitor		Component Firmware			Exploitation of Vulnerability	Graphical User Interface	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	
New Service		DLL Side-Loading	Credentials in Files	Local Network Configuration Discovery		InstallUtil			Custom Cryptographic Protocol
Path Interception		Disabling Security Tools	Input Capture		Logon Scripts	PowerShell	Data from Removable Media		
Scheduled Task		File Deletion	Network Sniffing	Local Network Connections Discovery	Pass the Hash	Process Hollowing		Exfiltration Over Command and Control Channel	Data Obfuscation
File System Permissions Weakness		File System Logical Offsets	Two-Factor Authentication Interception		Pass the Ticket	Regsvcs/Regasm	Email Collection		Fallback Channels
Service Registry Permissions Weakness				Network Service Scanning	Remote Desktop Protocol	Regsvr32	Input Capture	Exfiltration Over Other Network Medium	Multi-Stage Channels
Web Shell		Indicator Blocking		Peripheral Device Discovery	Remote File Copy	Rundll32	Screen Capture		Multiband Communication
Basic Input/Output System	Exploitation of Vulnerability				Remote Services	Scheduled Task	Audio Capture	Exfiltration Over Physical Medium	
Bootkit	Bypass User Account Control			Permission Groups Discovery	Replication Through Removable Media	Scripting	Video Capture		Multilayer Encryption
Change Default File Association	DLL Injection					Service Execution		Scheduled Transfer	Peer Connections
Component Firmware	Component Object Model Hijacking	Indicator Removal from Tools		Process Discovery	Shared Webroot	Windows Management Instrumentation			Remote File Copy
Hypervisor				Query Registry	Taint Shared Content				Standard Application Layer Protocol
Logon Scripts		Indicator Removal on Host		Remote System Discovery	Windows Admin Shares	MSBuild			
Modify Existing Service		InstallUtil		Security Software Discovery					Standard Cryptographic Protocol
Redundant Access		Masquerading		System Information Discovery					Standard Non-Application Layer Protocol
Registry Run Keys / Start Folder		Modify Registry		System Owner/User Discovery					Uncommonly Used Port
		NTFS Extended Attributes		System Service Discovery					Web Service
Security Support Provider		Obfuscated Files or Information		System Time Discovery					
Shortcut Modification									
Windows Management Instrumentation Event Subscription		Process Hollowing							
		Redundant Access							
Winlogon Helper DLL		Regsvcs/Regasm							
		Regsvr32							
		Rootkit							
		Rundll32							
		Scripting							
		Software Packing							
		Timestomp							
		MSBuild							
		Network Share Removal							

KEY

- Development
- Peer Review
- Partial Protection
- Full Protection

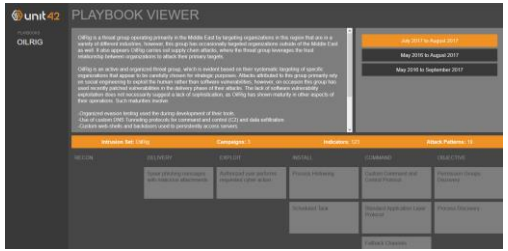
Development – 19

Peer Review – 2

#HIMSS18

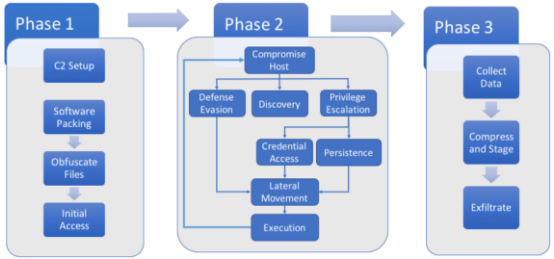
Future Vision: Threat-Informed Defense

CTI in ATT&CK

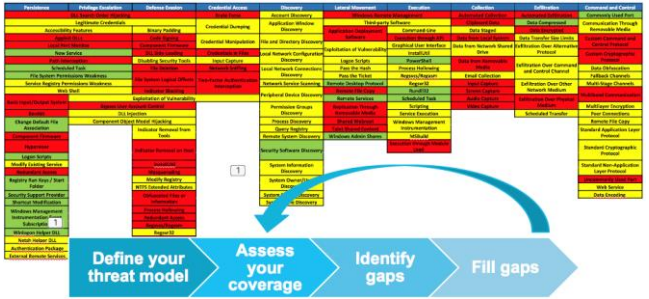


Realistic Threat Model

Intelligence-Driven Adversary Emulation



An ever-improving and well-validated defense



#HIMSS18

Take action

Figure out where you are

- Define your threat model in ATT&CK™.
- Assess your gaps. Ask your vendors.
- Are you where you want to be?

Figure out where to go and how to participate

- Can you use analytics now?
- Can you create analytics yourself?

Find a community to join

- Talk to your Information Sharing Analysis Organization/Center (ISAO/ISAC), vendors, partners, friends
- Find open source analytics

Resources

https://attack.mitre.org
attack@mitre.org
Twitter: @MITREAttack

What's next for ATT&CK™
https://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/whats-next-for-attck™

Analytic Repositories

- MITRE Cyber Analytic Repository: https://car.mitre.org
- ThreatHunter-Playbook: https://github.com/Cyb3rWard0g/ThreatHunter-Playbook
- Sigma: https://github.com/Neo23x0/sigma

Validation and Testing

- Atomic Red Team: https://github.com/redcanaryco/atomic-red-team
- Adversary Emulation Plans: https://attack.mitre.org/wiki/Adversary_Emulation_Plans

Questions

- Denise Anderson, President, NH-ISAC
  www.nhisac.org

- Julie Connolly, CISSP, MITRE
  jconnoll@mitre.org

NH-ISAC
NATIONAL HEALTH - ISAC

MITRE
www.mitre.org