#### H/MSS18 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<sup>™</sup>-Based Analytics**

Session 123, March 7, 2018

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

Julie Connolly, Principal Cybersecurity Engineer, MITRE





www.himssconference.org 🕑 in 🔊 #HIMSS18

DISCLAIMER: The views and opinions expressed in this presentation are those of the author and do not necessarily represent official policy or position of HIMSS.

MIMENI

This technical data was developed using contract funds under Basic Contract No. W15P7T-13-C-A802 Approved for Public Release; Distribution Unlimited. Case Numbers 18-0075, 17-4293-4 @2018 The MITRE Corporation. All Rights Reserved.

WHERE THE WORLD CONNECTS FOR HEALTH

# **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<sup>™</sup>) family of models
- Using ATT&CK™
- Collaborative ATT&CK<sup>™</sup> Analytics Development Effort



# **Learning Objectives**

- Explain the Adversarial Tactics, Techniques, & Common Knowledge (ATT&CK<sup>™</sup>) for Enterprise framework, as well as the broader family of ATT&CK<sup>™</sup> models, for characterizing post-compromise adversary behavior
- Describe how to use the ATT&CK<sup>™</sup> 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<sup>™</sup>- based analytics to detect post-compromise cyber attackers on healthcare systems and networks



# **Remember This?**







# **Threat Landscape**



The leading health information and technology conference

©HIMSS 2018



# **Threat Actors**

HUMSS 18 The leading health information and technology conference

#HIMSS18

©HIMSS 2018



# **Motivation**

The leading health information and technology conference

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



# **Motivation**

HUMSS<sup>18</sup> The leading health information and technology conference

©HIMSS 2018



# 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?



ne leading health information and technology conference

WHERE THE WORLD CONNECTS FOR HEALTH



-Mandiant, M-Trends 2017

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



# **Bianco's Pyramid of Pain**

*h*/mss<sup>-18</sup>

ne leading health information and technology conference

WHERE THE WORLD CONNECTS FOR HEALTH



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

# **Hard Questions**

 Image: The leading health information and technology conference

 WHERE THE WORLD CONNECTS FOR HEALTH

- 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<sup>™</sup>)

The leading health information and technology conferen

WHERE THE WORLD CONNECTS FOR HEALTH

# ATT&CK<sup>™</sup>

ATT&CK<sup>™</sup> 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



	E0-50	BAC4A2	IBE Z 5		07353	C			
9. D4DB0 325F3F A8			85B/0			7BAD898	30075078	DEC DEC	
80851	37B 660		05 2 B		20 43	89A 3		18/18	587B 66
	DLL Search Order Hijacking		Brute Force	Account Discovery	Windows Remo	te Management	Audio Capture	Automated Exfiltration	Commonly Used Port
Legitimate Credentials		Legitimate Credentials		Application Window	Third-party	Software	Automated Collection	Data Compressed	Communication Through
Accessibility	Features	Binary Padding	Credendar Dumping	Discovery	Application Deployment	Command-Line	Clipboard Data	Data Encrypted	Removable Media
AppInit	DLLs	Code Signing	Credential Manipulation	File and Directory Discovery	Software	Execution through API	Data Staged	Data Transfer Size Limits	Connection Proxy
Local Port	Monitor	Component Firmware	creacing manipulation	The and Directory Discovery	Exploitation of Vulnerability	Execution through Module	Data from Local System	Exfiltration Over Alternative	Custom Command and
New Se	ervice	DLL Side-Loading	Credentials in Files	Local Network Configuration	Exploration of vulnerability	Load	Data from Network Shared	Protocol	Control Protocol
Path Inter	rception	Disabling Security Tools	Input Capture	Discovery	Logon Scripts	Graphical User Interface	Drive	Exfiltration Over Command	Custom Cryptographic
Schedule	ed Task	File Deletion	Network Sniffing	Local Network Connections	Pass the Hash	InstellUtil	Data from Removable Media	and Control Channel	Protocol
File System Permis	ssions Weakness	File System Logical Offsets	Two-Factor Authentication	Discovery	Pass the Ticket	MSBuild			Data Encoding
Service Registry Perr	nissions Weakness		Interception	Network Service Scanning	Remote Desktop Protocol	PowerShell	Email Collection	Exfiltration Over Other	Data Obfuscation
Wahs	hall	Indicator Blacking			Pemote Ele Conv	Drocers Hollowing	Input Centure	Network Medium	Fallback Channels
Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command & Control
Desic input/output system		indicator Kemoval from Tools	A Fairman	Remote System Discovery	Windows Admin Shares	Service Execution			Standard Application Laver
Change Default File Association		Indicator Removal on Host	032BRRBC	Security Software Discovery	1 1201	Windows Management Instrumentation	17	3 7 6	Protocol Standard Cryptographic
Component Firmware	2000 Barris	Install Root Certificate	: 200750			ATT 1 9 97			Protocol
External Remote Services		InstallUtil	DOLLAD	System Information Discovery	001	Shill intert			
Hypervisor		Masquerading							Standard Non-Application
Logon Scripts		Modify Registry	7000	System Owner/User	OTCARS.	SED A A THE		2 8 9 6 6	
Modify Existing Service		MSBuild	A COLORED BY	Discovery	a prost in the local day			A CONTRACTOR OF MILL	Uncommonly Used Port
Netsh Helper DLL		Network Share Removal	And the same the	System Service Discovery					Web Service
Redundant Access		NTFS Extended Attributes	40.04169	System Time Discovery					
Registry Run Keys / Start Folder		Obfuscated Files or Information			1000	20A12	372931		
Security Support Provider		Process Hollowing				to the fail the short			
Shortcut Modification		Redundant Access							
Windows Management		Regsvcs/Regasm	THE ROOM	COLD CONTRACTOR		TICADO			7.0.0
Instrumentation Event		Regsvr32		and a subserve	- the Q at U / 1	10 / DM			3 4 20
Subscription		Rootkit			and the second			1 and and the second	
Winlogon Helper DLL		Rundll32			8 0 0 0 0 0			A CONTRACTOR	
		Scripting	and the second second		and the second of the second s				
		Software Packing	17 0 0 0		Acres 64				
		Timestomp	and the first state of the second						

:53D

#### Breaking Apart the ATT&CK<sup>™</sup> Model

The leading health information and technology conference

WHERE THE WORLD CONNECTS FOR HEALTH



#### 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

#### Adversary Tactics

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



# The ATT&CK<sup>™</sup> Model



The leading health information and technology conference

Persistence	Privilege Escalation	Defense Evasi <u>on</u>	Credential Acc <u>ess</u>	Discovery	Lateral Movem <u>ent</u>	Execution	Collection	Exfiltration	Command and Control	
	DLL Search Order Hijacking		Brute Force	Account Discovery	Windows Remo	te Management	Audio Capture	Automated Exfiltration	Commonly Used Port	
	Legitimate Credentials			Application Window	Third-party Software		Automated Collection	Data Compressed	Communication Through	
Accessibili	ty Features	Binary Padding	Credential Dumping	Discovery	Application Deployment	Command-Line	Clipboard Data	Data Encrypted	Removable Media	
Appin	it DLLs	Code Signing			Software	Execution through API	Data Staged	Data Transfer Size Limits	Connection Proxy	
Local Por	t Monitor	Component Firmware	Credential Manipulation	File and Directory Discovery		Execution through Module	Data from Local System	Exfiltration Over Alternative	Custom Command and	
News	New Service DLL Sid		Credentials in Files	Local Network	Exploitation of Vulnerability	Load	Data from Network Shared	Protocol	Control Protocol	
Path Interception		Disabling Security Tools	Input Capture	Configuration						
Schedu	led Task	File Deletion	Network Sniffing	Local Netw						
File System Perm	issions Weakness	File Sustem Legisel Offecte	T		round	d in ro	al data	fromo	whar inc	idante
Service Registry Pe	rmissions Weakness	File System Logical Offsets	I wo-Factor Authentication	Netwo,	nounae		al Uala			nuents
Web	Shell	Indicator Blocking		Parinharol D						
Authentication Package		Exploitation of Vulnerability	1	renpileral De						
	Bypass User A	ccount Control		Permission Groups	Replication Through	Regsvr32	Video Capture	Medium	Multiband Communication	
Bootkit	DLL In	jection	ļ	Discove			_			
Component Object Model		Component Object Model		Procer	nahlos	nivotir	na hotw	oon roc	toam a	and
Hijacking	-	Hijacking	4		nabies	ρινοιπ	Ig Delw	CEILIEL		IIIG
Basic Input/Output System		Indicator Removal from Tools		Remote S.	lue tea	m				
Change Default File Association		Indicator Removal on Host	]	Security Softwar		Instrumentation	1		Standard Cryptographic	
Component Firmware	1	Install Root Certificate	1		1	l			Protocol	
External Remote Services	ſ	InstallUtil	1	System Inf						
Hypervisor	ł	Masquerading	1	Ur .				•		1.
Logon Scripts	1	Modify Registry	1	Svs	)ecoun	les the	nroniei	m trom	the sol	ution
Modify Existing Service		MSBuild		<u>ь</u>						
Netsh Helper DLL	1	Network Share Removal	1	System Servic						
Redundant Access		NTFS Extended Attributes	]	System Time Discovery	1					
Registry Run Keys / Start	]	Obfuscated Files or	]		-					
Folder	ļ	Information	4		<b>T</b>			<b>f</b>		
Security Support Provider	Į	Process Hollowing	1		ransto	rms thi	nkind t	DV TOCUS	sina on	
Shortcut Modification	Į	Redundant Access	]							
Windows Management		Regsvcs/Regasm	4	ľ	DOST-PY	nioit ao	lversar	v hehav	lor	
Instrumentation Event		Regsvr32	4	1			i ci cui		101	
Subscription	{	Rootkit	4							
Winlogon Helper DLL	J	Rundli32	4							
		Scripting	{							
		SOTTWARE PACKING	1							
		Timestomp	1							<b>U</b> #HIM:
					10					
					10					©HIN
								© 2018 The	MITRE Corporation	วท

#### **Example of Technique Details – Persistence:** <u>New Service</u>

WHERE THE WORLD CONNECTS FOR HEALTH

**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:** <u>New Service</u> example <u>Hinss 18</u> The leading health information and technology conference (Continued)

#### Mitigation:

Limit privileges of user accounts and remediate <u>Privilege Escalation</u> 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<sup>™</sup> Use Cases**

WHERE THE WORLD CONNECTS FOR HEALTH

- 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

21



#### Threat Intel: What do you need **Himss 18** to worry about? (NOTIONAL)

Regsvr32

Rootkit

Rundll32 Scripting

Software Packing Timestomp

Winlogon Helper DLL

The leading health information and technology conference

WHERE THE WORLD CONNECTS FOR HEALTH

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 Remo	te Management	Automated Collection	Automated Exfiltration	Commonly Used Port		
Legitimate Credentials		Credential Dumping	Application Window Discovery	Third-part	y Software	Clipboard Data	Data Compressed	Communication Through		
Accessibility	/ Features	Binary Padding			Application Deployment	Command-Line	Data Staged	Data Encrypted	kemovable Media	
AppInit	DLLs	Code Signing	Crodential Manipulation	File and Directory Discovery	Software	Execution through API	Data from Local System	Data Transfer Size Limits	Custom Command and	
Local Port Monitor		Component Firmware	Credential Manipulation	File and Directory Discovery	Post - the March - CM - La constativity	Graphical User Interface	Data from Network Shared	Exfiltration Over Alternative	Control Protocol	
New Se	rvice	DLL Side-Loading	<b>Credentials in Files</b>	Local Network Configuration	Exploitation of vulnerability	InstallUtil	Drive	Protocol	Custom Cryptographic	
Path Inter	ception	Disabling Security Tools	Input Capture	Discovery	Logon Scripts	PowerShell			Protocol	
Schedule	ed Task	File Deletion	Network Sniffing	Local Network Connections	Pass the Hash	Process Hollowing	Data from Removable Media	Exfiltration Over Command and Control Channel	Data Obfuscation	
Service File Permis	sions Weakness	File System Logical Officets		Discovery	Pass the Ticket	Regsvcs/Regasm	Email Collection		Fallback Channels	
Service Registry Perr	nissions Weakness	File System Logical Offsets	I wo-Factor Authentication	Network Service Scanning	Remote Desktop Protocol	Regsvr32	Input Capture	Exfiltration Over Other Network	Multi-Stage Channels	
Web S	ihell	Indicator Blocking		Device and the Diversion	Remote File Copy	Rundll32	Screen Capture	Medium		
	Exploitation of Vulnerabilit			Peripheral Device Discovery	Remote Services	Scheduled Task		Exfiltration Over Physical	Multiband Communication	
Basic Input/Output System	Bypass User Acc			Bermissien Crowns Discovery	Replication Through Removable	Scripting	1	Medium	Multilayer Encryption	
Bootkit	DLL In	jection		Permission Groups Discovery	Media	Service Execution	1	Scheduled Transfer	Peer Connections	
				Process Discovery	Shared Webroot	Windows Management			Remote File Copy	
Change Default File Association		Indicator Removal from Tools		Query Registry	Taint Shared Content	Instrumentation			Standard Application Layer	
Component Firmware				Remote System Discovery	Windows Admin Shares				Protocol	
Hypervisor		Indicator Removal on Host		6					Standard Cryptographic	
Logon Scripts		InstallUtil		Security Software Discovery	j				Protocol	
Modify Existing Service		Masquerading		System Information Discovery					Standard Non-Application	
Redundant Access		Modify Registry								
Registry Run Keys / Start Folder		NTFS Extended Attributes		System Owner/User Discovery					Uncommonly Used Port	
		Obfuscated Files or							Web Service	
Security Support Provider		Information		System Service Discovery	J					
Shortcut Modification		Process Hollowing								
Windows Management Instrumentation Event		Redundant Access	White	e-shaded ce	lls have no ι	usage; darke	er cells have	more.		
Subscription		Regsvcs/Regasm								

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



# Measuring Defense: What can you cover? (NOTIONAL)

Network Share Removal

Install Root Certificate



he leading health information and technology conference

WHERE THE WORLD CONNECTS FOR HEALTH

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Moveme	nt Execution	Collection	Exfiltration	Command and Control	
DLL Search Order Hijacking			Brute Force	Account Discovery	Window	ws Remote Management	Automated Collection	Automated Exfiltration	Commonly Used Port	
Legitimate Credentials			Credential Dumping	Application Mindow Discovery	TI	hird-party Software	Clipboard Data	Data Compressed	Communication Through	
Accessibili	Accessibility Features		Credential Dumping	Application window Discovery	Application Deploy	ment Command-Line	Data Staged	Data Encrypted	Removable Media	
AppInit DLLs Local Port Monitor		Code Signing	Credential Meninulation	File and Directory Discovery	Software	Execution through API	Data from Local System	Data Transfer Size Limits Exfiltration Over Alternative	Custom Command and Control	
		Component Firmware	Credential Manipulation			Graphical User Interface	Data from Network Shared		Protocol	
New Service		DLL Side-Loading	Credentials in Files	Local Network Configuration	exploitation of vulnerability	InstallUtil	Drive	Protocol	Custom Countegraphic Protocol	
Path Inte	erception	Disabling Security Tools	Input Capture	Discovery	Logon Scripts	PowerShell	Data from Romovable Media		Custom Cryptographic Protocol	
Schedu	led Task	File Deletion	Network Sniffing	Local Network Connections	Pass the Hash	Process Hollowing	Data Holli Kelilovable Media	Exfiltration Over Command and Control Channel	Data Obfuscation	
File System Perm	issions Weakness	File System Logical Officets		Discovery	Pass the Ticket	Regsvcs/Regasm	Email Collection		Fallback Channels	
Service Registry Per	rmissions Weakness	File System Logical Onsets	I wo-Factor Authentication	Network Service Scanning	Remote Desktop Pro	otocol Regsvr32	Input Capture	Exfiltration Over Other Networ	Multi-Stage Channels	
Web	Shell	Indicator Blocking		Borinhoral Davice Discovery	Remote File Cop	y Rundll32	Screen Capture	Medium	Multihand Communication	
Pacie Input /Output System		Exploitation of Vulnerability		Peripheral Device Discovery	Remote Service	s Scheduled Task	Audio Capture	Exfiltration Over Physical	Multiballu communication	
Basic input/Output System	Bypass User A	ccount Control		Bermission Groups Discovery	Replication Through Re	movable Scripting	Video Capture	Medium	Multilayer Encryption	
Bootkit	DLL In	jection		Permission Groups Discovery	Media	Service Execution		Scheduled Transfer	Peer Connections	
Change Default File Association	Component Obje	ct Model Hijacking		Process Discovery	Shared Webroo	t Windows Management			Remote File Copy	
change belaut the Association		Indicator Removal from Tools		Query Registry	Taint Shared Cont	ent Instrumentation			Standard Application Layer	
Component Firmware		Indicator Nemoval Ironi Tools		Remote System Discovery	Windows Admin Sh	ares MSBuild			Protocol	
Hypervisor						Execution through Modu	e		Standard Cryptographic	
		Indicator Removal on Host		Security Software Discovery		Load			Protocol	
Logon Scripts		1								
Niodity Existing Service		InstallUtil		System Information Discovery					Standard Non-Application Layer Protocol	
Redundant Access		Masquerading			-					
Registry Run Keys / Start Folder		NITEC Extended Attributes		System Owner/User Discovery					Uncommonly Used Port	
Conveitu Curenort Drovidor		NTFS Extended Attributes		Sustan Canvia Discovery	-				Web Service	
Shortcut Modification		Obfuscated Files or Information		System Time Discovery	4				Data Encoding	
Shortcutwouncation		Process Hollowing		System time Discovery	J					
Windows Management		Process Hollowing								
Subscription		Reacting / Reacting								
Winlogon Helper DLL		Regsvc3/ RegdSm								
Netch Helper DLL		Rootkit								
Authentiestien Deck		Rundli32		Hig	n	Ned	NO NO			
		Scripting								
External Remote Services	1	Software Packing		Confide	anco (	Confidance	Confida	nco		
		Timestomp		Connue		connuence				
		MSBuild							#HIMSS18	

@HIMSS 2018

#### Prioritized ATT&CK Coverage Matrix (NOTIONAL)



The leading health information and technology conference

WHERE THE WORLD CONNECTS FOR HEALTH

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Mov	rement	Execution	Collection	Exfiltration	Command and Control
DLL Search Order Hijacking		Brute Force	Account Discovery	Wi	Windows Remote Management		Automated Collection	Automated Exfiltration	Commonly Used Port	
Legitimate Credentials			Cradential Dumping	Application Window Discovery	Third-party		y Software	Clipboard Data	Data Compressed	Communication Through
Accessibili	ty Features	Binary Padding	Credential Dumping	Application window Discovery	Application Deployment		Command-Line	Data Staged	Data Encrypted	Removable Media
AppInit DLLs Local Port Monitor		Code Signing	Constantial & Constantian	File and Directory Directory	Software		Execution through API	Data from Local System	Data Transfer Size Limits	Custom Command and Control
		Component Firmware	Credential Manipulation	File and Directory Discovery		ula ere biliter	Graphical User Interface	Data from Network Shared	Exfiltration Over Alternative	Protocol
New S	Service	DLL Side-Loading	Credentials in Files	Local Network Configuration	Exploitation of v	unerability	InstallUtil	Drive	Protocol	
Path Inte	erception	Disabling Security Tools	Input Capture	Discovery	Logon Sc	ripts	PowerShell			custom cryptographic Protocol
Schedu	led Task	File Deletion	Network Sniffing	Local Network Connections	Pass the I	Hash	Process Hollowing	Data from Removable iviedia	Extiltration Over Command	Data Obfuscation
File System Perm	issions Weakness	File Sustem Legisel Offecte		Discovery	Pass the T	icket	Regsvcs/Regasm	Email Collection		Fallback Channels
Service Registry Per	rmissions Weakness	File System Logical Offsets	Two-Factor Authentication	Network Service Scanning	Remote Deskto	p Protocol	Regsvr32	Input Capture	Exfiltration Over Other	Multi-Stage Channels
Web	Shell	Indicator Blocking	interception	Revision Device Discovery	Remote File	e Copy	Rundli32	Screen Capture	Network Medium	
Pasia Innut /Outnut Sustam		Exploitation of Vulnerability		Peripheral Device Discovery	Remote Se	rvices	Scheduled Task	Audio Capture	Exfiltration Over Physical	Monipand Communication
Basic input/Output System	Bypass User A	ccount Control		Permission Groups Discovery	Replication 1	Through	Scripting	Video Capture	Medium	Multilayer Encryption
Bootkit	DLL In	jection		Permission Groups Discovery	Removable	Media	Service Execution		Scheduled Transfer	Peer Connections
Change Default File Association	Component Obje	ct Model Hijacking		Process Discovery	Shared We	broot	Windows Management			Remote File Copy
change Default File Association		Indicator Romoval from Tools		Query Registry	Taint Shared	Content	Instrumentation			Standard Application Layer
Component Firmware		Indicator Removal from Tools		Remote System Discovery	Windows Adm	in Shares	MSBuild			Protocol
Hypervisor						Execution through Module				Standard Crysteeraphic
		Indicator Removal on Host		Security Software Discovery			Load	]		Protocol
Logon Scripts										
Modify Existing Service		InstallUtil		System Information Discovery						Standard Non-Application
Redundant Access		Masquerading				INC	Covorado			
Registry Run Keys / Start Folder		Modify Registry		System Owner/User Discovery						Uncommonly Used Port
Country Country Deviden		NIFS Extended Attributes				1000000000	000000000000000000000000000000000000000	000000000000000000000000000000000000000	00000000000000000	Web Service
Security Support Provider		Obfuscated Files or		System Service Discovery		Hia	h Confidence	e of Detection		Data Encoding
Shortcut Modification		Information		System Time Discovery		''''9				
Windows Management		Process Hollowing	1							
Instrumentation Event		Redundant Access			Moderate Confid			lence of Dete	ection	
Subscription		Regsvcs/Regasm								
Winlogon Helper DLL		Regsvr32								
Netsh Helper DLL		Rootkit				LOW	/ Confidence	of Detection		
Authentication Package		Rundli32								
External Remote Services		Scripting				Dric	ritized Adver	oon (Toobaia		
	-	Software Packing				PIIC	Auver	sary recriniq	ues	
		Timestomp								-
		MSBuild					ـ ا	aaad		#HIMSS18
		Network Share Removal					LE	egena		-
	Instal Root Certificate 24								©HIMSS 2018	

#### Using ATT&CK<sup>™</sup> to Improve Threat Intelligence-based Cyber Defense WHERE THE WORLD CONNECTS FOR HEALTH



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

HIMSS18

©HIMSS 2018

#### Sounds great, but how do I do this?

WHERE THE WORLD CONNECTS FOR HEALTH



🗹 Symantec Official Blog



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

Symantec Security Response

View Profile

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

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"

**IN[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!



WHERE THE WORLD CONNECTS FOR HEALTH

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			Crodontial Dumping	Application Window	Third-part	y Software	Clipboard Data Data Compressed		Communication Through
Accessibi	lity Features	Binary Padding	Credential Dumping	Discovery	Application Deployment	Command-Line	Data Staged	Data Encrypted	Removable Media
Аррі	nit DLLs	Code Signing	Credential Manipulation	File and Directory Discovery	Software	Execution through API	Data from Local System	Data Transfer Size Limits	Custom Command and
Local Port Monitor		Component Firmware	credential manipulation	File and Directory Discovery	Exploitation of Vulnorability	Graphical User Interface	Data from Network Shared	<b>Exfiltration Over Alternative</b>	Control Protocol
New	Service	DLL Side-Loading	Credentials in Files	Local Network Configuration		InstallUtil	Drive	Protocol	Custom Cryptographic
Path In	terception	Disabling Security Tools	Input Capture	Discovery	Logon Scripts	PowerShell	Data from Domoushie Modia		Protocol
Sched	uled Task	File Deletion	Network Sniffing	Local Network Connections	Pass the Hash	Process Hollowing	Data if officient wella	and Control Channel	Data Obfuscation
File System Perr	nissions Weakness	File System Logical Offsets	The Friday bull out of the	Discovery	Pass the Ticket	Regsvcs/Regasm	Email Collection		Fallback Channels
Service Registry Pe	ermissions Weakness	File System Logical Onsets	Interception	Network Service Scanning	Remote Desktop Protocol	Regsvr32	Input Capture	Exfiltration Over Other	Multi-Stage Channels
We	b Shell	Indicator Blocking	interception	Parinharal Davies Discovery	Remote File Copy	Rundll32	Screen Capture	Network Medium	Multihand Communication
People In must /Outmust Suptam		Exploitation of Vulnerability		Peripheral Device Discovery	Remote Services	Scheduled Task	Audio Capture	Exfiltration Over Physical	Wultiband Communication
sasic input/Output system	Bypass User A	ccount Control		Bermission Groups Discovery	Replication Through	Scripting	Video Capture	Medium	Multilayer Encryption
Bootkit	DLL Inj	jection		Permission Groups Discovery	Removable Media	Service Execution		Scheduled Transfer	Peer Connections
Change Default File	Component Object	ct Model Hijacking		Process Discovery	Shared Webroot	Windows Management			Remote File Copy
Association		Indicator Romoval from Tools		Query Registry	Taint Shared Content	Instrumentation			Standard Application Layer
Component Firmware				Remote System Discovery	Windows Admin Shares	MSBuild			Protocol
Hypervisor Logon Scripts		Indicator Removal on Host		Security Software Discovery		Execution through Module Load			Standard Cryptographic Protocol
Modify Existing Service		InstallUtil		System Information					Standard Non-Application
Redundant Access		Modify Registry		Custom Ourses/Use					Lincommonly Licod Port
Folder		NTES Extended Attributes		Discov					Web Service
Security Support Provider		Obfusional Files or		System 5 scovery					Data Encoding
Shortcut Modification				Svr Discovery					Data Liteounig
Mindau Manager		Process Hollowing		- Sy - Conscovery	1				
Windows Management		Redundant Access							
Subscription		Regsues /Regsem							
Winlogon Helper DI I		Regsvr32							
Netsh Helner DLL			J						
Authentication Package									
External Remote Services			$\mathbf{N}$ AS	<u>5855 _ `</u>					
External Remote Sel VICes	Deilr	ie vour							
	41			OUL				IOS	
	threa	tmode			Z da	DS /			
				erade /	ુ કુવ				
					28				

## **Start somewhere**

Scripting oftware Packin Timestom

HAMSS<sup>18</sup> WHERE THE WORLD CONNECTS FOR HEALTH

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 Remo	te Management	Audio Capture	Automated Exfiltration	Commonly Used Port		
Legitimate Credentials			Credential Dumping	Application Window	Third-party Software		Automated Collection	Data Compressed	Communication	ŀ
Accessibi	ity Features	Binary Padding	er ca	Discovery	Application	Command-Line	Clipboard Data	Data Encrypted	Media	
Appl	nit DLLs	Code Signing	Credential	File and Directory	Software	Execution through API	Data Staged	Data Transfer Size Limits	Connection Proxy	
Local Po	rt Monitor	Component Firmware	Manipulation	Discovery	Exploitation of	Execution through	Data from Local System	Exfiltration Over	Custom Command	
New	Service	DLL Side-Loading	Credentials in Files	Local Network	Vulnerability	Load	Data from Network	Alternative Protocol	and Control Protocol	
Path In	erception	Disabling Security Tools	Input Capture	Discovery	Logon Scripts	Graphical User Interface	Shared Drive	E-Elbertine Orea	Custom	
Sched	uled Task	File Deletion	Network Sniffing	Local Network	Pass the Hash	InstallUtil	Data from	Command and	Protocol	
File System Per	nissions Weakness	File System Logical		Discovery	Pass the Ticket	MSBuild	Removable Media	control channel	Data Encoding	
Service Registry Pe	rmissions Weakness	Offsets	Authentication	Network Service Scanning	Remote Desktop Protocol	PowerShell	Email Collection	Exfiltration Over	Data Obfuscation	
We	Shell		Peripheral Device		Remote File Copy	Process Hollowing	Input Capture	Medium	Fallback Channe	ĥ
Authentication	Authentication Bypass User Account Contro		1	Discovery	Remote Services	Regsvcs/Regasm	Screen Capture	Exfiltration Over Physical Medium	Multi-Stage Chanr	ĥ
Package Bypass User Ac		ecount control	_	Permission Groups	Replication Through	Regsvr32	Video Capture		Multiband	2
Bootkit	DLL Inj	jection		Discovery	Removable Media	Rundll32		Scheduled Transfer	Communication	
Component Object Mode Hijacking		Component Object Model Hijacking		Process Discovery	Shared Webroot	Scheduled Task			Mult A Encry	Į
Paris Input/ Output		Indicator Romoval		Query Registry	Taint Shared Content	Scripting	1		F Ve ppy	1
System		from Tools		Remote System Discovery	Windows Admin Shares	Service Execution			5 Indard A li	L
Change Default File Association		Indicator Removal on Host		Security Software Discovery		Windows Management Instrumentation			Standard Cryptographic Protocol	
Component Firmware External Remote Services Hypervisor		Install Root Certificate InstallUtil Masquerading		System Information Discovery					Standard Non-	
Logon Scripts		Modify Registry		System Owner/User					Protocol	
Modify Existing Service	]	MSBuild		Discovery					Uncommonly Used Port	
Netsh Helper DLL		Network Share Removal		System Service Discovery					Web Service	
Redundant Access		NTFS Extended Attributes		System Time Discovery						
Registry Run Keys / Start Folder		Obfuscated Files or Information								
Security Support Provide		Process Hollowing								
Shortcut Modification	1 1	Redundant Access								
Windows Management		Regsvcs/Regasm Regsvr32								
Instrumentation Event Subscription		Rootkit								
Winlogon Helper DLL	1 1	Rundil32								

Example: Sypass User count Control (T1088)



# Use what you have

 The leading health information and technology conference

 WHERE THE WORLD CONNECTS FOR HEALTH

- 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

©HIMSS 2018

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



Don't go

it alone!

WHERE **THE WORLD** CONNECTS FOR HEALTH

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



WHERE THE WORLD CONNECTS FOR HEALTH

0686

NH-ISAC Working group,

Healthcare companies

Dept. of Health & Human

Security vendors

Services (HHS)

led by Pfizer

• MITRE

**NH-ISAC Working Group:** Building out and sharing analytics to cover techniques in the ATT&CK<sup>™</sup> matrix

8 The MITRE Corporation

#### **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) The leading health information and technology conference WHERE THE WORLD CONNECTS FOR HEALTH

- 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 Winss 18 The Leading health Information and technology conference Next Steps



#HIMSS18 ©HIMSS 2018

#### **Future Vision: Threat-Informed Defense**

Dunit42 OILRIG

Phase 1

Obfuscate Files Initial Access HAMSS<sup>18</sup> The leading health information and technology conference

#### WHERE THE WORLD CONNECTS FOR HEALTH



# **Take** action

WMSS 18 The leading health information and technology conference WHERE THE WORLD CONNECTS FOR HEALTH

#### Figure out where you are

- Define your threat model in ATT&CK<sup>™</sup>.
- 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

WHERE THE WORLD CONNECTS FOR HEALTH

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

#### What's next for ATT&CK<sup>™</sup>

<u>https://www.mitre.org/capabilities/cybersecurity/</u> <u>overview/cybersecurity-blog/whats-next-for-</u> <u>attck</u>™

#### Analytic Repositories

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

#### **Validation and Testing**

- Atomic Red Team: <a href="https://github.com/redcanaryco/atomic-red-team">https://github.com/redcanaryco/atomic-red-team</a>
- Adversary Emulation Plans:

https://attack.mitre.org/wiki/Adversary\_Emulation\_Plans



WHERE THE WORLD CONNECTS FOR HEALTH

# Questions

- Denise Anderson, President, NH-ISAC <u>www.nhisac.org</u>
- Julie Connolly, CISSP, MITRE jconnoll@mitre.org





