

Tanium Endpoint Detection and Response

(ISC)² East Bay Chapter Training Day July 13, 2018

\$> WhoamI

• 11 Years of Security Experience

Multiple Verticals (Technology, Industrial, Healthcare, Biotech)

9 Years in Incident Response / Consulting

- Worked for 3 of the largest IR Consulting firms in the US
- Personally responded to over 150 active incidents in over 10 countries
- Several high profile / public data breach investigations
- Primary expertise in Digital Forensics, APT mitigation, Threat Intelligence

• Education:

BS, University of Central Florida

Certifications:

- SANS: GCFA, GCIH, GREM
- CISSP



The Old Way of Performing Incident Response The Traditional Approach Doesn't Scale

- · One of the security tools detects "something"
 - IDS signature, A/V hit, Threat Intelligence alert
- Reactive Approach
- Image the entire disk and/or dump memory
 - This takes a huge amount of time / Huge amount of data to analyze
 - 8-10 hours as most laptops are at least 500GB
 - Add another 12 hours for indexing with popular forensics tools
 - · Very effective, but not scalable for large incidents



It's Time to Re-think the Problem Statement

What Data is essential for Enterprise-scale incident response?

F TANIUM.



Matt Swann, https://github.com/swannman/ircapabilities

Logistics

- Lab environment URL
- Lab environment credentials
- Handouts
 - Slides
 - Lab supplements

Class outline

- Tanium Platform Overview
- Tanium Threat Response Workflow
- Hands on Labs



		•	•	•	•			•	•	•	٠	0																								
				•	•					•		•	•	•																						
														•	•	•																				
)																•	•	٠																		
)																•	•	•	•	•				•	•			•	•	•						
															•	•			•	•		•	•	•	•	۰			•	•						
																		•	•	•	•	•	•	•	•											
																															۰	•	•			
																															•	۰	•	•		
	•			•	•				•	•	•	•		•																				•	•	
	•		•	•	•	•	•	•	٠			•	•	•																						
			•	•	•	۰	•																													
			•	•	0														•	•				•	•											
																	•		•	•				•	•	•	•									
																			•	•					•	0										
																															•					

Tanium Platform Overview

Reviewing the basics

Tanium 101 Reviewing the basics

- Sensors
- Saved questions
- Actions

What's a sensor?

- "Ask a question" across all endpoints
- Search or collect data
 - "Live artifacts" native to the system
 - Evidence preserved by Tanium components (Index, Trace)
- Combine and "stack" common results for outlier analysis

uestion:	Get autoruns		
	Please select one of the f	ollowing queries:	
	Get AutoRun Program Detail	s from all machines	
	 Get Autoruns by Category 	y from all machines	3
	 Get Autoruns by Category Hash algorithm 	y from all machines	3
	 Get Autoruns by Category Hash algorithm Autoruns category 	y from all machines SHA256 System	3

Sensors can collect broad, unfiltered data...

List all loaded DLLs and their paths and hashes

1.0	n Linderten On II 07%		Cinar from Text Wrage	
	Loaded Modules with Hash[MD5]			
	Path 1	=	Hash 📃	Count 1 =
	C/Windows/aystem32/apphelp.dll		863/793d1504026b1a5fdeca873d4d84	65
0	C:Windows/ayetem02VATL.DLL		f1De5311e5093ta3c00f88c54c32fca	65
	C/Windows/aystem32/AUTHZ.dll		%54eb9352b7d898e9b3c2aa2ed724dad	65
h	C:Windows/wystem02%basesrv.DLL		dab748ae0459955ed21a22357533ddddb	65
	c:/windows/ayster/32/browser.dll		6e11f33d14d020f58d5e02e4d67dfa19	65
6	C/Windows/system321CFGMGR32.dll		3ftaea12005e565f51bf2fca674f543	65
	C/Windows/aystem32%CLBCatQ.DLL		#5688d308347f2720911d8796912834	65
ő	C:Windows/system321CLUSAPLDLL		ae9898ct5600a232ccd8ae3298682162e6	65
	C/Windows/aystem32/ongaudit.dll		50ba656134778a/64e4dd3c8b6fefd7e	65
6	C/Windows/aystem32/CRVPT32.dll		454e292001a4e/1d72943942bba/0917	65

Or they can take parameters to find specific items...

Index Query File Details Using Name[java*] File Size (Bytes) File Path T Creation Date Last Modification File MD5 Hash File Magic 2015-09-29 2015-09-29 C:\Program Files (x86)\Java\jre7\bin\javaw.exe 431b3f716a156dd628 4D5A9000 175528 19:04:22 19:04:22 2015-09-29 2015-09-29 C:\Program Files (x86)\Java\jre7\bin\javaws.exe 272808 a1f71601e9578a7b49 4D5A9000 19:04:22 19:04:22 2015-09-29 2015-09-29 C:\Program Files (x86)\Java\/re7\bin\/ava_crw_demo.dll 23976 0ce8105fb7cf990667£ 4D5A9000 19:04:22 19:04:22 2015-09-29 2015-09-29 C:\Program Files (x86)\Java\/re7\Ib\/avafx.properties 29 670fd7ff0f62ac0239ec 6A617661 10-04-22 10-04-00

Find any file on disk starting with the name "java"

You can "drill down" on results to ask follow-up questions

Se	elect Drilldown Question					
Sa	aved Questions Create a Ques	stion Build a	Question			
1	get computer name and operatin	g system			Q	Search
					Drill Down	Cancel
2 (10	C Dril Down	Deploy Action	More -	Filter by Computer Group *	Contains	 Filter by Te
	e Opdatoe: 0ff 🚺 100% (100% a					
	Scheduled Tasks					
	Task Name † 2		=	Command		= 0
	Ec2ConfigMonitorTask			%ProgramFiles%\Amazon\Ec2Co	nfigService\Ec20	ConfigMonitor.(8
	Googlel Indiate Taxis MachineCore			C:\Program Files (x86)\Google\I	Indate\GoogleU	odate exe /c 8

"Compound" questions combine output from multiple sensors

Que	stion: Get	Com	pute 3 Sys	r Name and Operating item containing "winds	Syste	m and Scheduled Tasks from inver*	ail m	achines with Q. Search				
	Save 1	is ques	tion (Copy to Question Builder						y		O dı
6am 8 p	totaŭ.							Filter by Computer Group *	Contains	100	by Test	્ય
Lie	Updatus: On]	100	94					Own	flot: Te	VI Wrotz -		
-						Scheduled Tasks						
	Computer Nam	1=	=	Operating System	=	Task Name	=	Command				=
0	AlphaDB.Training	com		Windows Server 2008 R	2 Stand	Ec2ConfigMonitorTask GoogleUpdateTaskMachineUA GoogleUpdateTaskMachineCore		NProgramFiles/WVmazor/Ec2Config5e C1Program Files (x86)/Google/Update// C1Program Files (x86)/Google/Update//	ervice/Ec2Cx GoogleUpda GoogleUpda	onfigMonitor.ex to.exe /ua./inst te.exe /o	a alsource	scheduler
.0	AlphaPC.Training	.com		Windows Server 2008 R	2 Starsc	Ec2ConfigMonitorTask At1 GoogleUpdateTaskMachineUA GoogleUpdateTaskMachineCore		16ProgramFilesWiAmazon/Ec2ConfigBi omd.exe /o.c1drop.exe C1/Program Files (x86)/Google/Update// C1/Program Files (x86)/Google/Update//	ervice/Ec2Cx GoogleUpda GoogleUpda	onflightfonition.ex to.exe Ava. Anet to.exe Ac	alacurce	scheduler

TANIUM

Tanium provides several tools to help you discover sensors

Ask a Question		Question Builder
Enter a question here.	/ou can use plain English.	Q Search
	Browse Sensors	
	Select a Category	Select a Sensor
	Type here to filter Category	Type here to filter Sensor
	Incident Response	Account Lockouts Security Event Log Search
	Index	Alternate Data Streams Job Results
	Java	AutoRun Program Details
	Kaspersky	Autoruns by Category
	Location	Browser Cookie Search
	Maintenance	Cleared Windows Security Event Log Search
	Mahlan	

"Saved Questions" collect data over time

estion:	Get	AutoRur	n Prog	ram Details co	ontaining "\Us	ers" from all machin	nes		Q Sear
	Save this	s question	Copy	to Question Build	er				
New Sav	ved Que	stion					Create Save	d Question	Cancel
Details									
	Name:	Autorun	s in Use	r Directories					
Que	stion Text:	Get Autol from all n	Run Pro nachine	gram Details cont s	aining "\Users"				
Setting	5								
C Re	strict this que	istion to only	y owner a	nd administrators		Default Tab:	Grid	•	
🗆 Ma	ke this quest	tion available	for drilld	OIMTI		Default Grid Chart Zoom:	Current	*	
C Ma	ke this quest	tion available	for merg	ing			Use these	settings as th	e default for
					-		Use these all users	settings as th	he default fo

Dashboards group together saved questions



F TANIUM.

What's an action?

- Change the state of a system
- Distribute a package of files and run a command
- Can target system(s) from any set of question results
- Can run once, or recur over time



Common actions for Threat Response workflows

- Quarantine host (isolate on the network)
- Launch IR Gatherer
- Kill process
- Edit registry
- · Edit hosts file
- Patch system

Deployment Package Select a package to deploy to the selected m	achines:
Apply Windows IPsec Quarantine	
Browse Packages	
Override Config	0
	Override Quarantine Configuration
Allow All DHCP	
Allow All DNS	
Allow All Tanium Servers	0 0
Validate Tanium Server Availability	0
Notification Message	Ø
Custom Quarantine Rules	IN:UDP:127.0.0.1:32:161 OUT:UDP:127.0.0.1::162

Training Lab: Practicing Basic Questions

Use "Ask a Question" in <u>Interact</u> to discover sensors and complete this lab

Practicing basic sensor questions

- 1. What operating systems are present in the demo environment?
- 2. What is the IP address of hostname "AlphaPC"?
- 3. Do any systems have Google Chrome as an installed application? What version?
- 4. Who is the last logged in user on client-1?
- 5. How many systems are listening for connections on port 3389? What are their hostnames?

Threat Response Workflow

a a a a a a a



TANIUM







Tanium Threat Response

Sources of evidence



Incident Response content searches native sources of evidence



Index provides full-disk search for file metadata

File hashes

MD5: fc5e038d38a57032085441e7fe7010b0 SHA1: 6adfb183a4a2c94a2f92dab5ade762a47889a5a1 SHA256: 936a185caaa266bb9cbe981e9e05cb78cd732b0b3...

File name and path

C:\temp\salary.xlsx

Tanium Index

File magic number

4D 5A 00 02

File timestamps

Created: 2015-05-09 10:09:43 Modified: 2015-05-09 10:20:01

G TANIUM.

Trace continuously records historical data

Filesystem events

- User & process context
- Type of event (Create, Delete, Rename, Write)

Registry events

- User & process context
- Type of event (key created, key deleted, value set, value deleted)

Process execution

- User context
- Command line & parent
- Hash
- Time created & terminated

Tanium Trace Recorder

Network connections

- Type of connection
- Remote & local port and IP
- DNS query and response
- User & process context

Driver loads

- User & process context
- Path
- Hash
- Digital signature

Security events

- Based on OS audit policy
- Logon / logoff, policy change, account and group changes, etc.

		٠	•	•	•			•	•	•		•																										
)				•	•					•		•	•	•																								
														•	•	•																						
															•	•	•	•																				
																٠	•	•	•	•				•	•			•	•	•								
									0						•	•		•	•	٠		۰	•	•	•	•			•	•								
												•	•	•				•	•	•	•	•	•	•	•						•		•	•	•	•	•	•
•	•				•	•				•	•	•	•			•	•	•			•		•								•	•	•	•	•	•	•	
	•	•	•	•	•	•			•	•	•	•	•	•	•						•										•				•	•		
	•		۰	٠	•	•	•	•	•			•	•	٠																								
			۰	٠	٠	•	•							•				•						•														
			•	٠	٠													•	•	٠	•	•	•	•	•	•					•							
																	•	•	•	•			•	•	•	•	•											
																			٠	•					•	•		•	•		•							
																															•	•				•	•	
																															•	•		•	•	•	•	•

.

Detection and alerting

Introducing Tanium Detect 3.0

Detection methods



F TANIUM.

Basic navigation Detect homepage and alerts

• Filter by

- Computer Name
- Match Details (artifact in an alert)
- Label
- Intel Name

Status

- Unresolved
- In Progress
- Resolved

	TANIUM					Bullet 7.0.314.0010 UK	1.0.0.6601
	Alerts						
			Status:	Unresolved In Progress	· Permit	Order By: 4 Alert Time	
	Filter Besulta						
	Computer Name:	Metch Detaile:		Label		Intel Name:	
	Filter by Computer Name	Filter by Match Details.		Piter by Label		Filter by Intel Name	
	*I AlphaWeb.Training.com	found misc, web, shells var via Artifact i	at Rest on N	ov 15. 8:45 PM			
	File c:\inetpub\www.	wroot\listart.aspa	as reast on the	or 10, 0.45 F M			
	AlphaWeb.Training.com	found grizzley_steppe_websheil.yar via	Artifact at P	est on Nov 15, 7:12 PM			
	File c:\inetpub\www.	root\grissly.php					
_	*I AinhaBC Training com l	ound backoff, yar via Running Processes	on Nov 15,	7:04 PM			
	a Aprile C. Hannig Com						

		, The second sec					Ť																													
•	•	•	•	•			•	•	•	•	•																									
			•	•					•	•	•	•	•																							
													•	•	•																					
															•	•	•																			
															•	•	•	•	٠				•	•			•	•	•							
													•	•	•			•	•			•	•	•				•	•							
													•				•	•	•	•	•	•	•	•												
				•							•	•																								
									•				•							•																
			Ť	, Ť	Ť	Ĭ																														
		•	•	٠														•	•	•			•	•												
																•	•	•	•			•	•	•	•	•										
																		•	•					•	۰		•	•	•	•						
																														•	•			•	•	
																														•	•	•	•	•	•	
		C																												•	•	•	•	•	•	•
						6		5																									•		•	



- Continuously monitor endpoint activity using Trace
- Detect any combination of file, process, network, or registry events
- Issue alerts to the Tanium console within seconds of a signal "match"

process.path ends with 'certutil.exe'
AND (process.command_line contains 'decode' OR process.command_line
contains '-urlcache')

file.operation is create AND
(file.path ends with '.vbs' OR
file.path ends with '.ps1') and
process.path contains 'winword.exe'

What's in a signal alert?

(+) AlphaPC.Training.com found Mimikatz Command Arguments via Tanium Signals on Nov 14, 12:29 PM
Process C:\Users\Administrator\Desktop\mimikats_trunk\x64\mimikats.exe
Process Command Line
mimixats privilege: debug sexurisa: logonpasswords
Process MDS
099120ACA1C34E7A529838390CFD8C1E
Process ID
4396
Parent Command Line
"C:\Windows\system32\cmd_exe"
Parent Process Id
4188
Process Anosstry
@ smss.exe -> @ smss.exe -> @ winlogon.exe -> @ userinit.exe -> @ explorer.exe -> @ cmd.exe -> A minikatr.exe
Tanium Signal Definition
process.command_line contains 'sekurlsa::'
View Advanced Details



2

Filter Results	Investigate in Trace
Showing: 73 of	Delete
Alphal	C Training com found Mimikatz Co

Establish Live Connection		×
Before we are able to investigate in Trace we need to inform Trace that we want a When the connection is complete the "Start live connection with AlphaPC.Training	live connection. g.com" button below will be enabled.	
🛛 New Browser Tab	Start live connection with AlphaPC.Training.com	Cancel

Signal alerts are linked to the corresponding process instance in Trace, allowing you to easily pivot into the complete forensic history around an event.

O Trace	< Live	Endpoint - AlphaPC mikatz.exe(4396) created by ALPHAPC\Ad	dministrator
Home	Sack	to search results	
Live Endpoints	Pro	ocess Details:	Save process eviden
Saved Evidence	Proc	ess Patr: Isens'Administrator'/Desktop'/mimikatz_trunk\x64'/mimikatz.exe	Process Command Line: mimikatz privilegeodebug
Enterprise Hunting	Proc	ess Hauh: 999120aca1c34e7a529b3b390cfdbc1e	Parent Command Line: *C:\Windows\system32\cmd.exe*
	Proc 439	ena ID: B	Parent Process ID: 4188
	UTC 201	Time Created: 7-11-14 20:29:14.563	UTC Time Terminated: 2017-11-14 20:30:09.467
	User Adm	inistrator	

•	•	٠	•	•			•	•	•	•	•																									
			•	•					•		•	•	•																							
													•	•	•																					
															•	•	٠																			
															•	•	•	•	•			•	•			•	•	•								
														•	•			•	•	•	•	•	•	•			•	•								
																													•		•	•	•	•	•	•
•				•					•	•	•	•			•														•		•	•	•	•		
•		•	•	•	•			•	•	•	•	•	•	•															•				•	•		
•	•	•									, T																									
		۰	•	٠	•	•							•									•														
			•															•	•				•													
																•	•	•	•			•	•	•	•											
																		٠	٠				•	•			•		•							
																																		•		
																													•	•		•	•	•	•	•

Investigating with Trace

.

• •

Tanium Trace Key Components

- Recorder: Continuously preserve endpoint activity via kernel-level monitoring
- Sensors: Search Trace data across all systems via "Ask a question"
- Workbench: Web UI for investigation tasks (single-host and enterprise)



20 May 2015 File (32)
Registry (3)
Network
Process (14)
05:14
05:15
05:16
05:17
Wed May 20 2015 05:15:35.911: Connection attempted. (172.16.11.137:50358 to 199.27.75.133:443)

What does Trace record?

Windows and Linux

Process execution

- User context
- Command line
- Parent command line
- Hash
- Time created & terminated

File system

- User & process context
- Type of event (Create, Delete, Rename, Write)

Registry (Windows-only)

- User & process context
- Type of event (key created, key deleted, value set, value deleted)

Network Connection

Type of connection event

- Remote & local port and IP
- User & process context

DNS (Server 2012R2 / Win8.1 & later)

- Queried domain
- Response IP
- Initiating process

Security

- · Based on current audit policy
- Can include: logon, logoff, lockout, auth. policy change, account and group changes
- Driver load
 - User & process context
 - Path
 - Hash
 - Digital signature

Single-host analysis workflow



Lab: Investigating an Office Macro Attack

Open the Trace snapshot for **client-1**: Trace \rightarrow Saved Evidence \rightarrow Snapshots

Do not use a live connection for this lab.

Search for process **Z4U8K1S8.EXE** – drill down and pivot from there to answer the following questions

1. What processes did EXCEL.EXE launch (aside from **Z4U8K1S8.EXE)**?

- 2. What was the purpose of the "certutil.exe" command? What did it do?
- 3. After initiating a command shell, what commands did the attacker execute?
- 4. What was the file name of the original malicious Excel document that led to the infection?

G TANIUM.

What processes did EXCEL.EXE launch (aside from Z4U8K1S8.EXE)?

Z4U8K1S8.exe(3256) created by TAM\alphauser								
Back to search results								
Process Details:	Vow: 🎟 🕯							
Save process evidence								
Process Path:	Process Command Line:							
C:\Users\alphauser\AppData\Roaming\Microsoft\AddIns\Z4U8K1S8.exe	C:\Users\alphauser\AppData\Roaming\Microsoft\AddIns\Z4U8K1S8.exe							
Process Hash:	Parent Command Line:							
C6685E9C908A991EEF4857792D0A724E	*C:\Program Files\Microsoft Office\Root\Office16\EXCEL.EXE* /dde							
	•							
	Q Q Reset							
0 33	68: EXCEL.EXE							
3380: EXCEL.EXE O 0 79	2: certutil.exe							

TANIUM

What was the purpose of the "certutil.exe" command? What did it do?

Back to search results	
Process Details:	View: III 4
Save process evidence	
Process Path:	Process Command Line:
C:\Windows\System32\certutil.exe	certutil -decode
	C:\Users\alphauser\AppData\Roaming\Microsoft\AddIns\T1U3H6N7.txt
	C:\Users\alphauser\AppData\Roaming\Microsoft\AddIns\Z4U8K1S8.exe
Process Hash:	Parent Command Line:
B72B52259E744B7C2D174FC69D422D83	"C:\Program Files\Microsoft Office\Root\Office16\EXCEL.EXE" /dde

certutil.exe(792) created by TAM\alphauser

The macro launched "certutil.exe" to extract the malware payload, "Z4U8K1S8.EXE", from temporary file "T1U3H6N7.TXT"

TANIUM

After Z4U8K1S8.EXE initiated a command shell, what commands did the attacker execute?

Process (2)			
.643			
Fri Dec 16 2016 23:1	10:01.643:	Connection atte	mpted. (10.10.10.135:49244 to 10.10.10.129:4444)
Detailed Process H	listory		
1 - 3 of 3 results			Double click a child process row to view
Add Evidence Remov	e Evidence		
Export to Excel			
Timestamp +	Type 🕤	Operation 🕤	Detail
2016-12-16 23:10:01.198	Process	CreateProcess	3256: C:\Users\alphauser\AppData\Roaming\Microsoft\AddIns\Z4U8K1S8.exe
2016-12-16 23:10:01.643	Network	Connection atte	10.10.10.135:49244 to 10.10.10.129:4444
2016-12-16 23:10:52.024	Process	CreateChild	1588: C:\Windows\System32\cmd.exe



TANIUM

What was the file name of the original malicious Excel document that led to the infection?

Search File events for ".xls" files created by "outlook.exe" (in Excel ancestry)

xpiore by:	Combine	a Driver	File	Network	Process	Registry	Security	
Path	¢ c	ontains	¢	Search fo	or			Add

Process Path	Operation	User	Path
C:\Program Files\Microsoft Office\	Write	alphauser	C:\Users\alphauser\AppData\Loca\Microsoft\Windows\INetCache\Content.Outlook\7R7DAD5S\Florase Portal Setup (002).xis:Zone.Identifier
C:\Program Files\Microsoft Office\	CreateNewFile	alphauser	C:\Users\alphauser\AppData\Loca\Microsoft\Windows\iNetCache\Content.Outlook\7R7DAD5S\Florase Portal Setup (002).xls:Zone.Identifier
C:\Program Files\Microsoft Office\	CreateNewFile	alphauser	C:\Users\alphauser\AppData\Local\Microsoft\Windows\iNetCache\Content.Outlook\7R7DAD5S\Florase Portal Setup (002).xls
C:\Program Files\Microsoft Office\	CreateNewFile	alphauser	C:\Users\alphauser\AppData\Loca\Microsoft\Windows\iNetCache\Content.Outlook\7P(7DAD5S\Florase Portal Setup (002).xls
C:\Program Files\Microsoft Office\	CreateNewFile	alphauser	C:\Users\alphauser\AppData\Locs\Microsoft\Windows\INetCache\Content.Outlook\7R7DAD5S\Florase Portal Setup.xis:Zone.Identifier
C:\Program Files\Microsoft Office\	Write	alphauser	C:\Users\alphauser\AppData\Local\Microsoft\Windows\/NetCache\Content.Outlook\7R7DAD5S\Florase Portal Setup.xis
C:\Program Files\Microsoft Office\	CreateNewFile	alphauser	C:\Users\alphauser\AppData\Loca\Microsoft\Windows\/NetCache\Content.Outlook\/7R7DAD5S\/Florase Portal Setup.xis
C:\Program Files\Microsoft Office\	CreateNewFile	alphauser	C:\Users\alphauser\AppData\Loca\Microsoft\Windows\iNetCache\Content.Outlook\7R7DAD5S\Florase Portal Setup.xis

F TANIUM.

Next steps...

What didn't we cover today?