

LESSONS LEARNED ON ATTACK DETECTION IN THE CLOUD

Nick Jones – ISF Denmark – September 2021

WHO AM I?

Nick Jones

- Senior Security Consultant @ F-Secure
- Global cloud security lead
- Working on:
 - Attack Detection
 - Cloud security at scale
 - DevSecOps & security automation



AGENDA



GRENT INSTRACTATIO DEFECTION





ON-PREMISE VS CLOUD

HOW CLOUD DETECTION DIFFERS

UNCERTAINTY OF MALICIOUS INTENT

Fewer actions in the cloud are obviously bad compared to on-premise, making generic detection rules harder

CONTEXT IS KEY

LABS

Anomalies will vary by environment. Behavioral analytics are important here, so is developing environment-specific alerting.

GAINING VISIBILITY IS EASIER

Org-wide CloudTrail, etc. makes it easier to gain visibility into much of your estate. Shadow IT now the primary issue, rather than coverage of known assets.



ATTACKERS ARE AUTOMATING

Attackers leveraging scripted attacks to abuse stolen credentials for cryptocurrency mining. With an API-driven attack surface by-design, it's easier to automate targeted attacks too.

MINDSET SHIFT



CERTAINTY OF MALICIOUS INTENT

CONTEXT IS KEY



ON-PREMISE TELEMETRY



CLOUD TELEMETRY

Control Plane Telemetry





DESIGNING YOUR CLOUD DETECTION STACK

CENTRALISE EVERYTHING



DATA SOURCES

SOURCE	BENEFIT
Control Plane audit logs (CloudTrail, Audit Log etc)	Visibility of all administrative actions
Cloud-native detection services	Detection of known bad activity
API Gateway/WAF Logs	Identify malicious requests to applications
Network flow logs	Identify anomalous traffic by source and destination, volumes etc
System logs from any VMs	Grants OS-level visibility of potential attacker activity
Endpoint Detection and Response agents in VMs	Detects malicious activity within VMs as with on premise estates
Application logs	Provides app-specific contextual information
Service Specific Logs (storage access logs, function executions, KMS key access etc)	Shows access and usage of specific resources and services, which may help to track lateral movement or actions on objective



THE THREAT INTELLIGENCE PROBLEM

ON-PREMISE VS CLOUD DETECTION





LABS

ENTERPRISE CLOUD ADOPTION



ENTERPRISE VS CLOUD ATT&CK

Reconnalssance 10 techniques	Resource Development 6 techniques	Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 15 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting	Account Manipulation (4)	Abuse Elevation Control	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected	Application	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public- Facing Application	Exploitation for Client	BITS Jobs	Access Token	Access Token Manipulation (5)	from Password Stores (3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (s)	External Remote Services	Execution Inter-Process	# Autostart Execution (12)	Manipulation (5) Boot or Logon	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Through Removable Media	Exfiltration Over	Data Encrypted for Impact
Gather Victim Network Information (t)	Develop Capabilities (c)	Hardware Additions	Communication (2)	Boot or Logon Initialization	Autostart Execution (12)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session	Clipboard Data	Data Encoding (2)	Protocol (3)	Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts m	Phishing (I) Replication	II Scheduled Task/Job so	Scripts (1) Browser Extensions	Boot or Logon Initialization Scripts in	Direct Volume Access	Forge Web Credentials	Cloud Service Dashboard	Hijacking (2) Remote	Data from Cloud Storage Object	Data Obfuscation (7)	Exfiltration Över C2 Channel	Defacement (2) Disk Wipe av
Phishing for Information (II)	Obtain Canabilities (c)	Through Removable Media	Shared Modules	Compromise Client	Create or Modify System	Modification (2)	II Input Capture (4)	Domain Trust Discovery	Services (II) Replication	Data from Configuration Repository	Dynamic Resolution (3)	Exfidention Over Other Network	Endpoint Denial
Search Closed Sources (7)	copuonica (s)	Bupply Chain Compromise (3)	Software Deployment Tools	Create	Process (4)	Exploitation for Defense	Man-in-the- Middle (2)	File and Directory Discovery	Through Removable Media	Data from	Encrypted Channel (2)	Medium (1)	Firmware
Search Open Technical Databases (5)		Trusted Relationship	System Services (2)	Create or Modify	Modification (2)	File and Directory	Modify Authentication	Network Service Scanning	Software Deployment Tools	Repositories (2)	Fallback Channels	Over Physical Medium (1)	Inhibit System
Search Open Websites/Domains (D		II Valid Accounts (4)	Windows	Process (ii)	Execution (15)	Modification (2)	Network Sniffing	Network Sniffing	Taint Shared Content	System	Transfer	Exfiltration Over Web	Network Denial
Search Victim-Owned Websites			Management Instrumentation	Event Triggered Execution (15)	Privilege Escalation	Hide Artifacts (7) Hijack Execution	OS Credential Dumping (0)	Password Policy Discovery	Use Alternate Authentication	Data from Network Shared Drive	Channels	Scheduled	Resource Hijacking
				External Remote Services	Hijack Execution Flow (11)	Flow (11)	Steal Application Access Token	Peripheral Device Discovery	Material (4)	Data from Removable Media	Non-Application Layer Protocol	Transfer Transfer Data to	Service Stop
				Hijack Execution Flow (11)	Process Injection (11)	Indicator Removal on	Steal or Forge	Permission Groups Discovery (3)		Data Staged (2)	Non-Standard Port Protocol Tunneling	Cloud Account	System Shutdown/Reboot
				Implant Container Image	Scheduled Task/Job (6)	Indirect Command	Tickets (4)	Process Discovery		Collection (3)	Proxy (4)		
				Office Application Startup (6)	Valid Accounts (4)	II Masquerading (II)	Cookie	Remote System Discovery		Man in the Browner	Remote Access Software		
				Pre-OS Boot (5)		n Modify Authentication Process (4)	Authentication	II Software Discovery (1)		Man-in-the- Middle (2)	Traffic Signaling (1)		
				Task/Job (6)		Modify Cloud Compute Infrastructure (4)	Unsecured Credentials (6)	System Information Discovery		Screen Capture	Web Service (3)		
				Component (3)		Modify Registry		System Network Configuration Discovery		Video Capture			
				Signaling (1)		Network Boundary		System Network Connections Discovery					
				Valid Accounts (4)		Bridging (1) Obfuscated Files or		System Owner/User Discovery					
						Information (1)		System Service Discovery					
						II Process Injection (11)		II Virtualization/Sandbox					
						Rogue Domain Controller		Crasion (3)					
						Signed Binary Proxy							
						Signed Script Proxy							
						Subvert Trust							
						Template Injection							
						II Traffic Signaling (1)							
						Utilities Proxy Execution (1)							
						Unused/Unsupported Cloud Regions							
						Use Alternate Authentication Material (4)							
						Valid Accounts (4)							
						Il Virtualization/Sandbox Evasion (3)							
						Weaken Encryption (2)							
						the soup roceandy							

Initial Acc 5 techniqu	es Stechniques	Privilege Escalation 2 techniques	Defense Evasion 6 techniques	Credential Access Stechniques	Discovery 9 techniques	Lateral Movement 2 techniques	Collection 4 techniques	Exfiltration 1 techniques	Impact 4 techniques
Drive-by Comprom	ise Account Manipulation (8)	Domain Policy	Domain Policy Modification (1)	Brute Force (4)	Account Discovery (2)	Internal Spearphishing	Data from Cloud Storage	Transfer Data to Cloud Account	II Defacement (1)
Exploit Public-Faci	ng Create Account (1)	= Valid Accounts	Impair Defenses (2)	Forge Web Credentials (2) Steal Application Access	Cloud Infrastructure	Use Alternate Authentication	Data from Information		II Endpoint Denial of Service (3)
Approation	Implant Container Image	Valid Accounts (2)	Modify Cloud Compute		Discovery	Material (2)	Repositories (2)		II Network Denial of Service (2)
Phishing (1)	Office Application Startup	-	Infrastructure (4)	Token	Cloud Service Dashboard		Data Staged in		Resource Hijacking
Trusted Relationsh	ip	(4)	Unused/Unsupported Cloud	Steal Web Session Cookie	Cloud Service Discovery		Emell Collection		
Valid Accounts	2)		Regions	II Unsecured Credentials (2)	Network Service Scanning		Email Collection (2)		
-		Use Alternate Authentication Material (2)			Permission Groups				
			Valid Accounts (2)		(i)	-			
					Software Discovery (1)				
					System Information Discovery				

System Network Connections Discovery



LABS



WHAT'S AN ATTACKER LIKELY TO DO?









LYBS

01

HOW DO I START?

Threat model your environment, identify attack paths and likely attacker actions

Prioritise attack paths and actions

Pick the most important attack paths, codify them

Verify telemetry is available to defenders

Execute attacker actions as kill chains, verify detection cases work as expected.

05

WHERE DO I START?



LEARN FROM DEVOPS: TREAT EVERYTHING AS CODE



Detection as code makes internal and external knowledge sharing easier



SIGMA (SIEM-agnostic rules)

https://github.com/Neo23x0/sigma

Jupyter Notebooks

https://posts.specterops.io/threat-hunting-with-jupyternotebooks-part-1-your-first-notebook-9a99a781fde7



John Lambert – The Githubification of Infosec

http://youtu.be/B3o-9z3Eitg

https://medium.com/@johnlatwc/the-githubification-ofinfosec-afbdbfaad1d1



LEONDAS

LEONIDAS

Automated Attack Simulation

- Framework for defining, executing and detecting attacker TTPs in the cloud
- Execution and detection all defined as code
- TTPs linked to MITRE ATT&CK for easy correlation with TI/existing tooling

Framework automatically generates...

- Executor serverless function
- Sigma detection rules
- Documentation

Executor

- Multi-cloud support in a single instance
- User/role/service account impersonation

LEONIDAS



CONTINUOUS INTEGRATION





CONCLUSIONS

DETECTION IS A JOURNEY





Context is key, use it to your advantage



Cloud environments change, your detection will too



Codify use cases (and attacks) to aid knowledge sharing

LEONIDAS





Automate attacker actions in the cloud



Both test and detection cases



AWS support now, Azure/GCP on the roadmap



41 test cases - more to come



https://github.com/fsecurelabs/leonidas