THE Zombie App-ocalypse

START!

Game Theory for Disrupting Dormant and Orphaned Cloud Identities

JOSHUA BAHIRVANI
SENIOR SECURITY RESEARCHER

SHALEEN DEV PK
SENIOR SECURITY RESEARCHER

Non-HUMAN IDENTITES

Non-Human Identities (NHIs) are machine-based identities used by applications, services, and automation in cloud environments.
Examples: Service accounts, API keys, certificates, workload identities, bots.

Why are NHIs Important?

- Power automation, integrations, and cloud-native workloads.
- Often have **higher privileges** than human users.
- **Outnumber human identities** in most cloud environments.

how to play

There are 3 different types of games APTs play !

Compromised App

Malicious App

Dormant App

SaaS MATRIX

INITIAL ACCESS	EXECUTION	PersIstENCE	PRIVILEGE ESCALATION	Defence EVASION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT	COLLECTION	EXFIL	IMPACT
Phishing	Serverless Exec	Account Manipulation	Account Manipulation	EXPLOITATION	Brute force	Account discovery	Internal spearPhishing	Automated collection	ALT PROTOCOL	Access Removal
Trusted Relationships	SDT	Create account	Event Triggered exec	IMpersonation	FOrge WEB Creds	cloud service dash	SDT	Cloud storage	WEb Service	FINANCIAL Theft
Valid Accounts		Event Triggered exec	Valid accounts	MODIFY Auth process	MODIFY Auth process	Cloud service discovery	TAINT Shared content	REPOS	CLOUD Account	resource hijacking
		MODIFY Auth process		Alt Auth	MFA request Generation	Passwordpolicy	Alt Auth			
		Valid accounts		Valid accounts	STEAl App Access Token	Permission groups				
					STEAl web session cookie					
					unsecured creds					

Attack moVES

INITIAL ACCESS	EXECUTION	PersIstENCE	PRIVILEGE ESCALATION	Defence EVASION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT	COLLECTION	EXFIL	IMPACT
Valid Accounts	Serverless Exec	Valid Accounts	Valid Accounts	Alt EXPLOITATION Auth	unsecured Brute force creds	Account discovery	Internal spearPhishing	Automated collection	ALT PROTOCOL	Access Removal
Phishing		Account Manipulation	Account Manipulation							
Trusted Relationships T1078 .004 Valid	SDT	T1078 Create account .004	T1078 Triggered exec .004	IMpersonation T1550 .001	FOrge WEB T1552 Creds .001	cloud service dash	SDT	Cloud storage	WEb Service	FINANCIAL Theft
		Event Triggered exec	Valid accounts	MODIFY Auth process	MODIFY Auth T1552 .005	Cloud service discovery	TAINT Shared content	REPOS	CLOUD Account	resource hijacking
		MODIFY Auth process		Alt Auth	MFA request	Passwordpolicy	Alt Auth			
		Valid accounts		Valid accounts	STEAl App Access Token STEAl App Access Token T1528 STEAl web session cookie	Permission groups				
					unsecured creds					

APT A

Attack moVES

INITIAL ACCESS	EXECUTION	PersIstENCE	PRIVILEGE ESCALATION	Defence EVASION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT	COLLECTION	EXFIL	IMPACT
Valid Accounts	Serverless Exec	Valid Accounts	Valid Accounts	Alt Auth	unsecured creds	Account discovery	Alt Auth	Automated collection	ALT PROTOCOL	Access Removal
T1078 .004	SDT	T1078 .004	T1078 .004	T1550 .001	T1552 .001	T1087 .004	T1550 .001	REPOS	WEb Service	FINANCIAL Theft
					T1552 .005			T1213 .003	CLOUD Account	resource hijacking
					STEAl App Access Token					
					T1528					

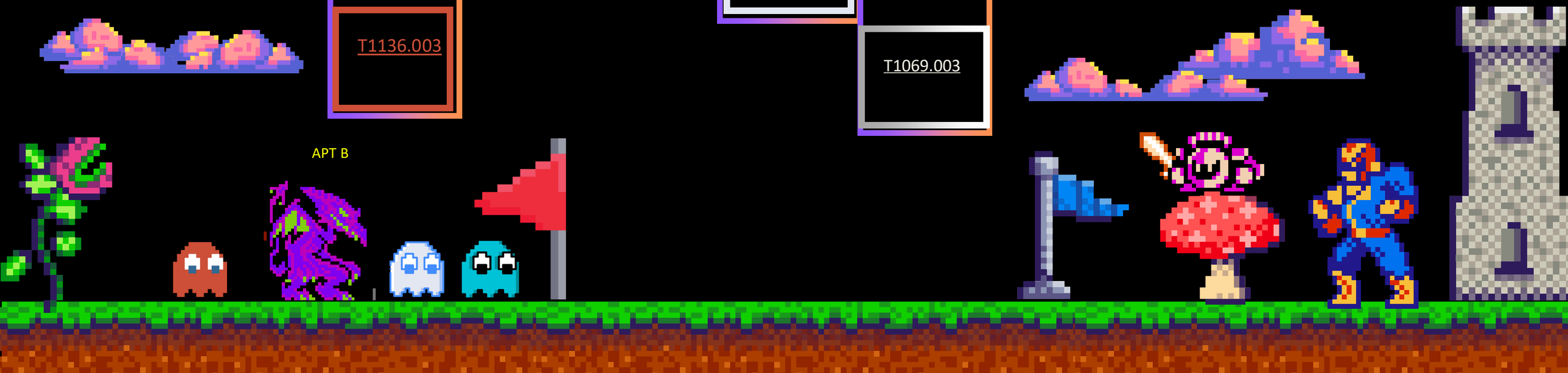
Attack moVES

INITIAL ACCESS	EXECUTION	PersIstENCE	PRIVILEGE ESCALATION	Defence EVASION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT	COLLECTION	EXFIL	IMPACT
Valid Phishing Accounts	Serverless Exec	Valid Account Manipulation Accounts	Valid Account Manipulation Accounts	Valid EXPLOITATION Accounts	Creds from pwd Brute force stores	Account discovery	Internal spearPhishing	Automated collection	ALT PROTOCOL	Access Removal
Trusted Relationships T1078 .004 Valid	SDT	Create account T1078 .004 Event Triggered exec Create Account	T1098.001 Event Triggered exec Valid accounts	IMpersonation T1078 .004 MODIFY Auth process Alt Auth Valid accounts	FOrge WEB T1555.006 Creds MODIFY Auth T1552 .005 MFA request Generation STEAl App Access Token STEAl web session cookie unsecured creds	cloud service T1087 .004 Cloud service discovery Permission group discovery Passwordpolicy T1069.003 Permission groups	SDT TAINT Shared content Alt Auth	Cloud storage REPOS	WEb Service CLOUD Account	FINANCIAL Theft resource hijacking
		MODIFY Auth process T1136.003 Valid accounts								

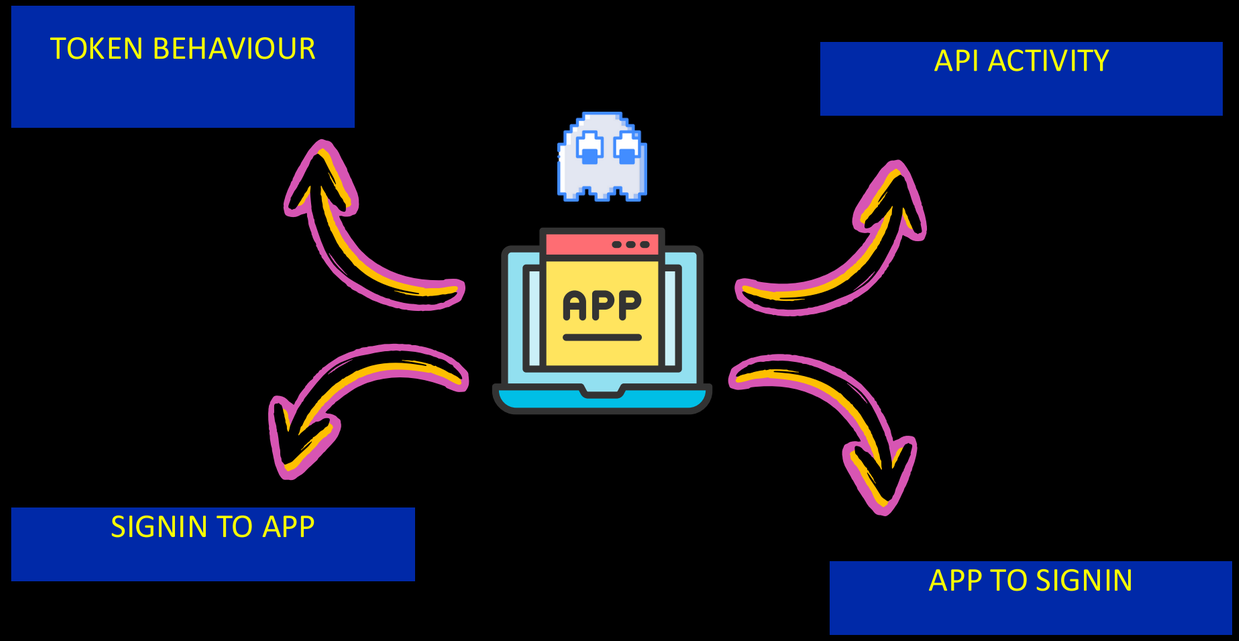
APT B

ATTACK Moves

INITIAL ACCESS	EXECUTION	PersIstENCE	PRIVILEGE ESCALATION	Defence EVASION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT	COLLECTION	EXFIL	IMPACT
Valid Accounts	Serverless Exec	Valid Accounts	Valid Accounts	Valid Accounts	Creds from pwd stores	Account discovery	Alt Auth	Automated collection	ALT PROTOCOL	Access Removal
T1078 .004	SDT	T1078 .004	T1098.001	T1078 .004	T1555.006	T1087 .004	T1550 .001	cloud APIs	WEb Service	FINANCIAL Theft
		Create Account			T1552 .005	Permission group discovery		T1119	CLOUD Account	resource hijacking
		T1136.003				T1069.003				



NHI DORMANCY



non-human identities that were previously in use but have not been used for a significant period

DETECTION Moves

INITIAL ACCESS	EXECUTION	PersIstENCE	PRIVILEGE ESCALATION	Defence EVASION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT	COLLECTION	EXFIL	IMPACT
Valid Accounts	Serverless Exec	Valid Accounts	Valid Accounts	Alt Auth	unsecured creds	Account discovery	Alt Auth	Automated collection	ALT PROTOCOL	Access Removal
T1078 .004	SDT	T1078 .004	T1078 .004	T1550 .001	T1552 ~~.001~~	T1087 .004	T1550 .001	REPOS	WEb Service	FINANCIAL Theft
					T1552 .005			T1213 .003	CLOUD Account	resource hijacking
					STEAl App Access Token					
					T1528					

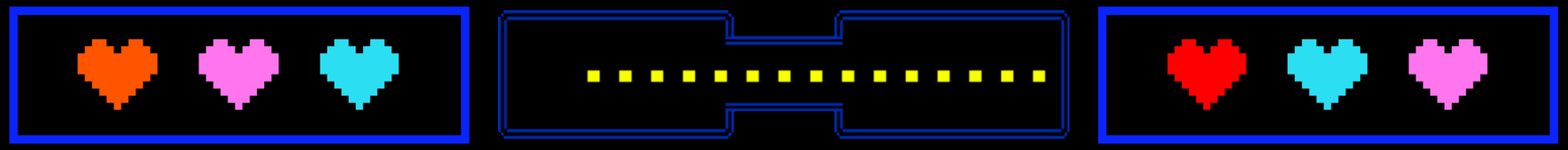
APT A

DETECTION Moves

INITIAL ACCESS	EXECUTION	PersIstENCE	PRIVILEGE ESCALATION	Defence EVASION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT	COLLECTION	EXFIL	IMPACT
Valid Accounts	Serverless Exec	Valid Accounts	Valid Accounts	Valid Accounts	Creds from pwd stores	Account discovery	Alt Auth	Automated collection	ALT PROTOCOL	Access Removal
T1078 .004	SDT	T1078 .004	T1098.001	T1078 .004	T1555.006	T1087 .004	T1550 .001	cloud APIs	WEb Service	FINANCIAL Theft
		Create Account			T1552 .005	Permission group discovery		T1119	CLOUD Account	resource hijacking
		T1136.003				T1069.003				

BEYOND DETECTION

DISRUPTION



HOW IS DISRUPTION DIFFERENT FOR AN NHI ?

OAuth application ID - Global representation of the application

Service principal of the application - Local representation of the application

Multitenant application - A service principal is created in each tenant where a user has consented to its use

Owners – OAuth application and Service Principal can have different owners

Now what exactly do we disrupt?

Grueling game

Any move that endangers the king is a wrong move

LET THE GAMES BEGIN

GAME THEORY

A comprehensive framework for disrupting Non-Human Identities (NHIs) with a phased approach is essential. This framework aims to curtail the threat actor's ability to exploit these applications throughout the Attack Tactics while minimizing the impact on users and business operations. Our goal is to be part of the team that defeats the attacker by taking the right set of disruption actions.

LET THE GAMES BEGIN

CHOOSE YOUR WEAPON

- Remove application secret 
- Delete Service Principal 
- Delete application 
- Remove Service Principal creds 
- Disable sign-ins from the Service Principal 

- Revoke API permissions
- Revoke Access Tokens 
- Disable sign-ins to the Service Principal 
- Revoke App Role Assigment from the app 
- Revoke unnecessary high permissions 

DISRUPTION Moves

INITIAL ACCESS	EXECUTION	PersIstENCE	PRIVILEGE ESCALATION	Defence EVASION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT	COLLECTION	EXFIL	IMPACT
Valid Accounts	Serverless Exec	Valid Accounts	Valid Accounts	Alt Auth	unsecured creds	Account discovery	Alt Auth	Automated collection	ALT PROTOCOL	Access Removal
T1078 .004	SDT	T1078 .004	T1078 .004	T1550 .001	T1552 .001	T1087 .004	T1550 .001	REPOS	WEb Service	FINANCIAL Theft
					T1552 .005			T1213 .003	CLOUD Account	resource hijacking
					STEAl App Access Token					
					T1528					

APT A

DISRUPTION moves

INITIAL ACCESS	EXECUTION	PersIstENCE	PRIVILEGE ESCALATION	Defence EVASION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT	COLLECTION	EXFIL	IMPACT
Valid Accounts	Serverless Exec	Valid Accounts	Valid Accounts	Valid Accounts	Creds from pwd stores	Account discovery	Alt Auth	Automated collection	ALT PROTOCOL	Access Removal
T1078 .004	SDT	T1078 .004	T1098.001	T1078 .004	T1555.006	T1087 .004	T1550 .001	cloud APIs	WEb Service	FINANCIAL Theft
		Create Account			T1552 .005	Permission group discovery		T1119	CLOUD Account	resource hijacking
		T1136.003				T1069.003				

Challenges

L E V E L U P

1:5 ratio of human identities to non-human identities (NHI) is leveraged for Business Email Compromise (BEC) and phishing attacks

Disruptions to be shifted to the early phases based on identified NHI attack paths

Clustering of NHIs across multiple tenants

GAME ON

END

QUESTIONS ?