

Emerging Cloud Security Threats

Cutting-Edge Detection Approaches

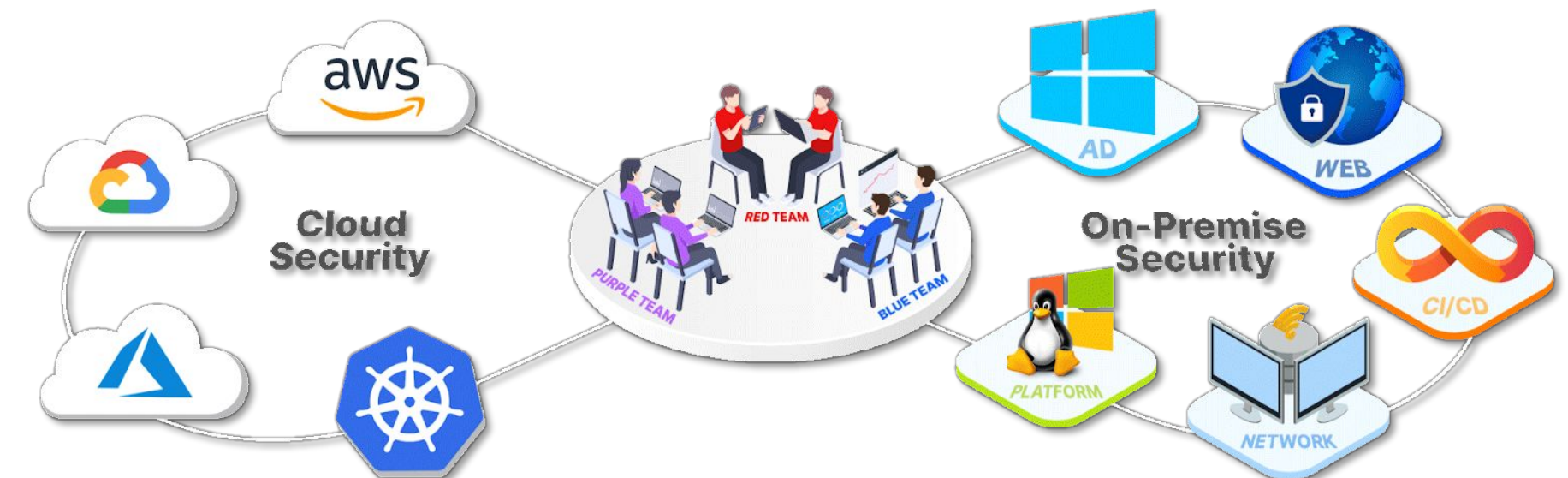
cyberwarfare.live



About CyberWarFare Labs :

CW Labs is a renowned Infosec company specializing in cybersecurity practical learning. They provide on-demand educational services. The company has 3 primary divisions :

1. Learning Management System (LMS) Platform
2. CWL CyberSecurity Playground (CCSP) Platform
3. Infinity Learning Platform



INFINITE LEARNING EXPERIENCE

About Speaker :

Harisuthan S

Senior Security Engineer

He Is a Blue Team Security researcher, bringing over 3+ years of experience in cyber defence. possesses a deep understanding of Blue Team methodologies including investigation and detection over cyber attacks.

Table of Content

1

Cloud Threat Landscape

3

Mitre Cloud Matrix

2

APTs targeting cloud

4

Conclusion

Cloud Threat Landscape 2025

1

Initial Access

- Phishing
- Valid Account
- Exploit Public Facing Application

2

Execution

- Cloud Command Line Tool

3

Privilege Escalation

- Account Manipulation

Cloud Threat Landscape 2025

4

Persistence

- External Remote service
- Create Account

5

Defense Evasion

- Impair Defense

6

Discovery

- Enumerating User/Group/Role/Policies
- Enumerating Cloud resources

Cloud Threat Landscape 2025

4

Credential Access

- Stored Credential
- Unsecure Credential

5

Collection

- Data Exfiltration

6

Impact

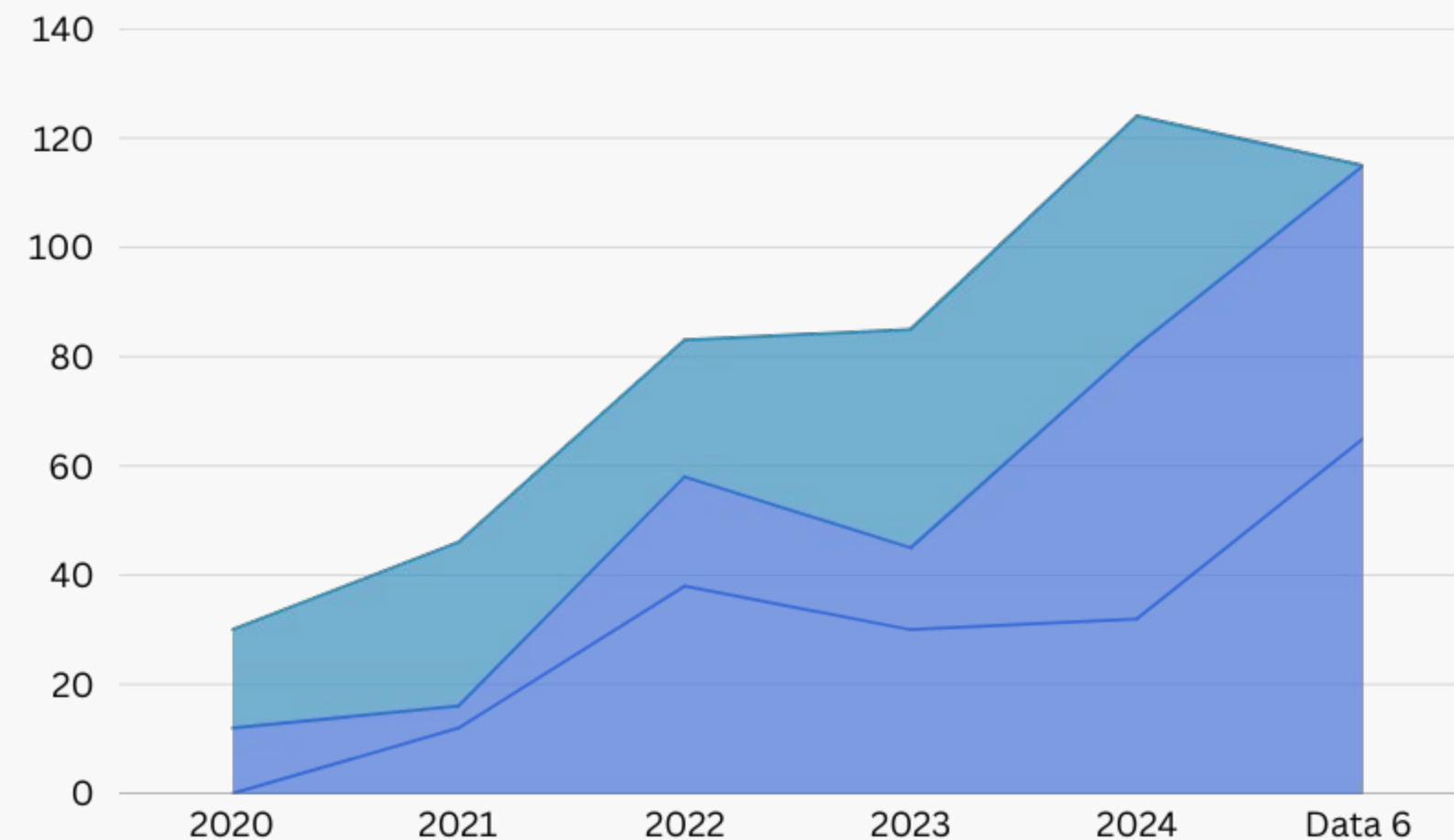
- Resource hijacking
- Data Encryption/destruction

Cloud breaches statistics

80% of companies have been subject to cloud security breaches.

27% of organizations experienced a public cloud security incident

62% of organizations reported they were either somewhat or highly likely to experience a cloud data breach in the next year.



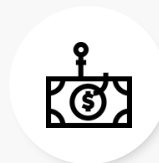
Emerging Cloud Security Threats



**IMDS Credential
Access**



**Resource
Hijacking**



**Cloud-Specific
Ransomware**

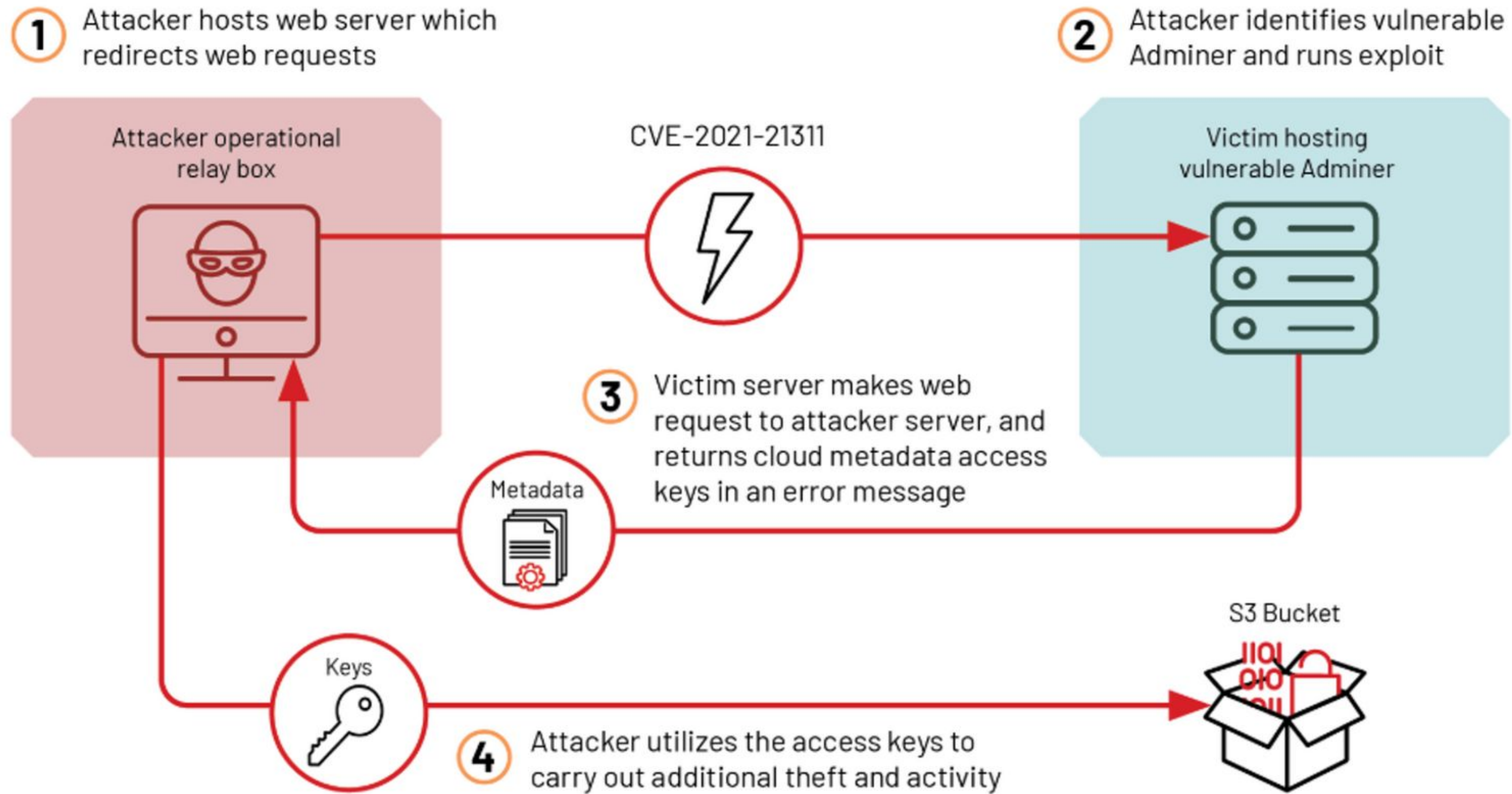


**Data
Destruction**

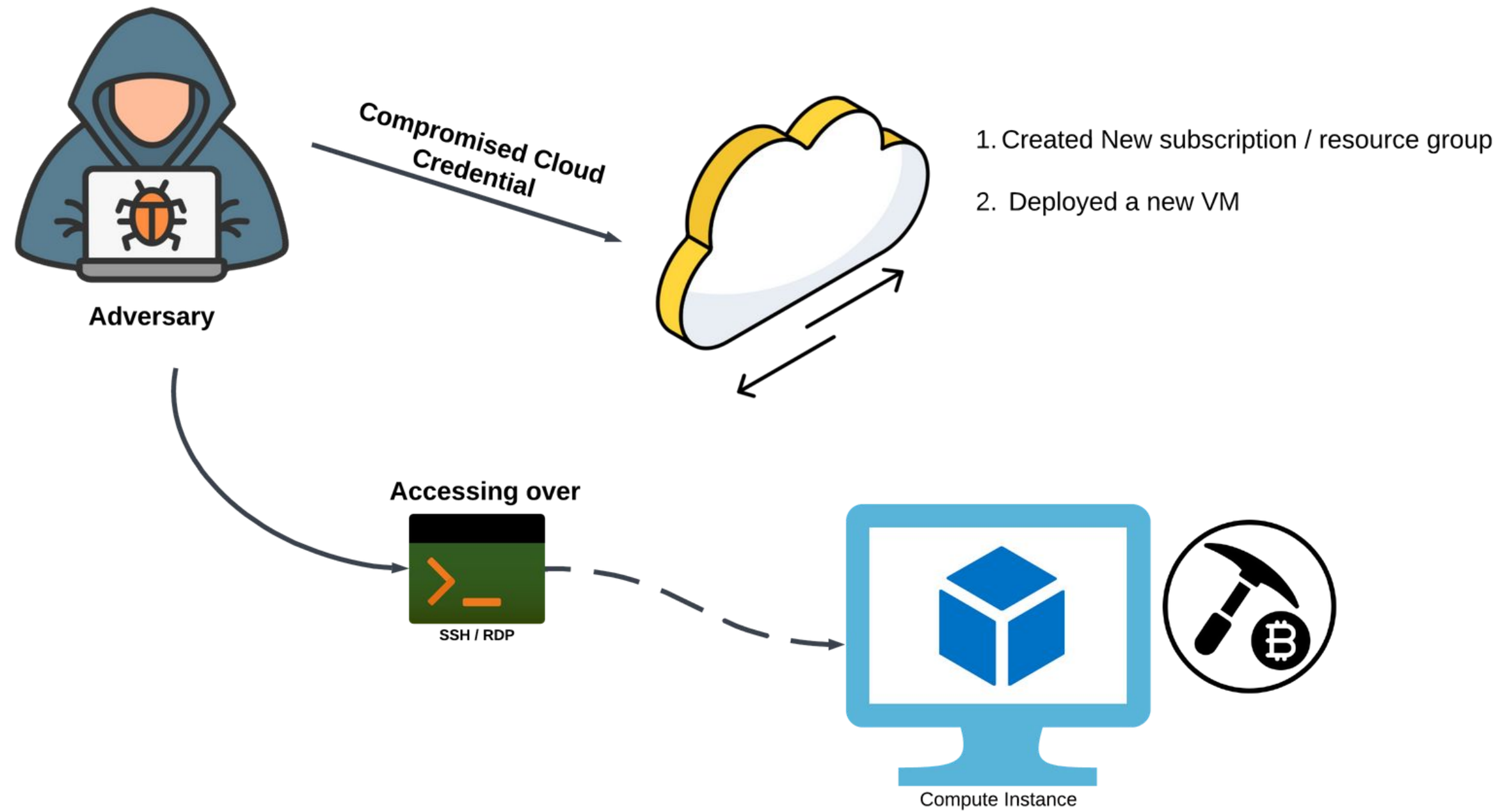


**Hijacking GenAI
infrastructure**

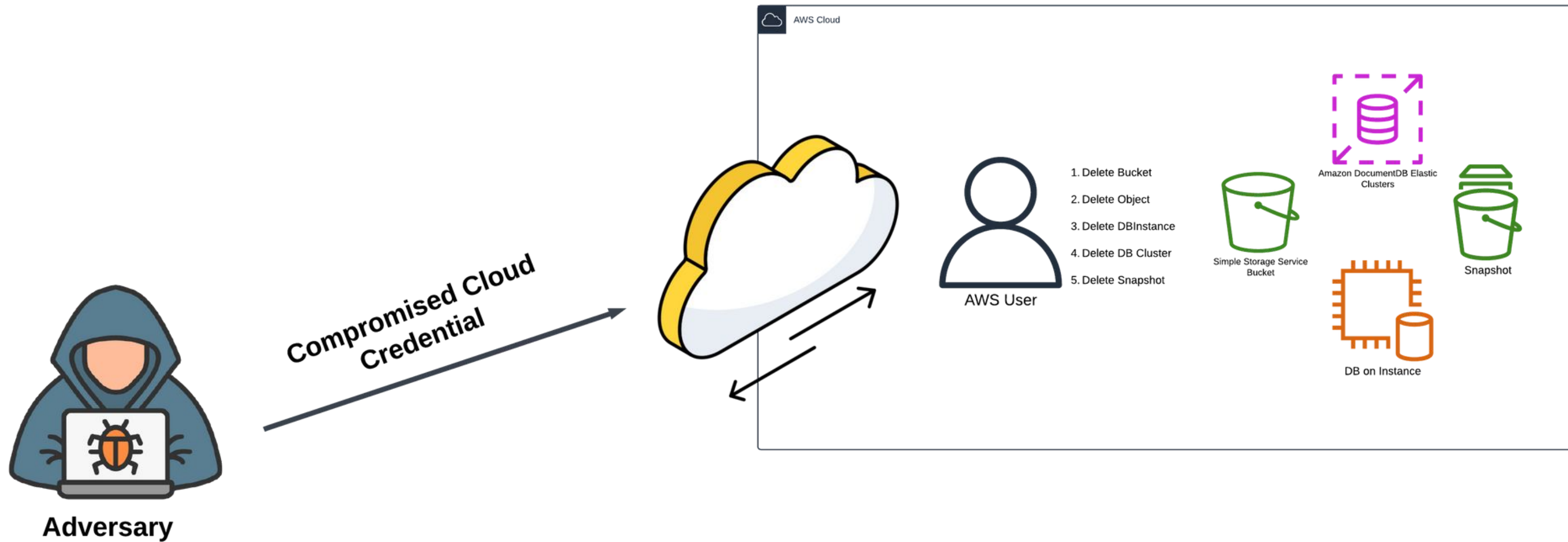
IMDS Credential Access



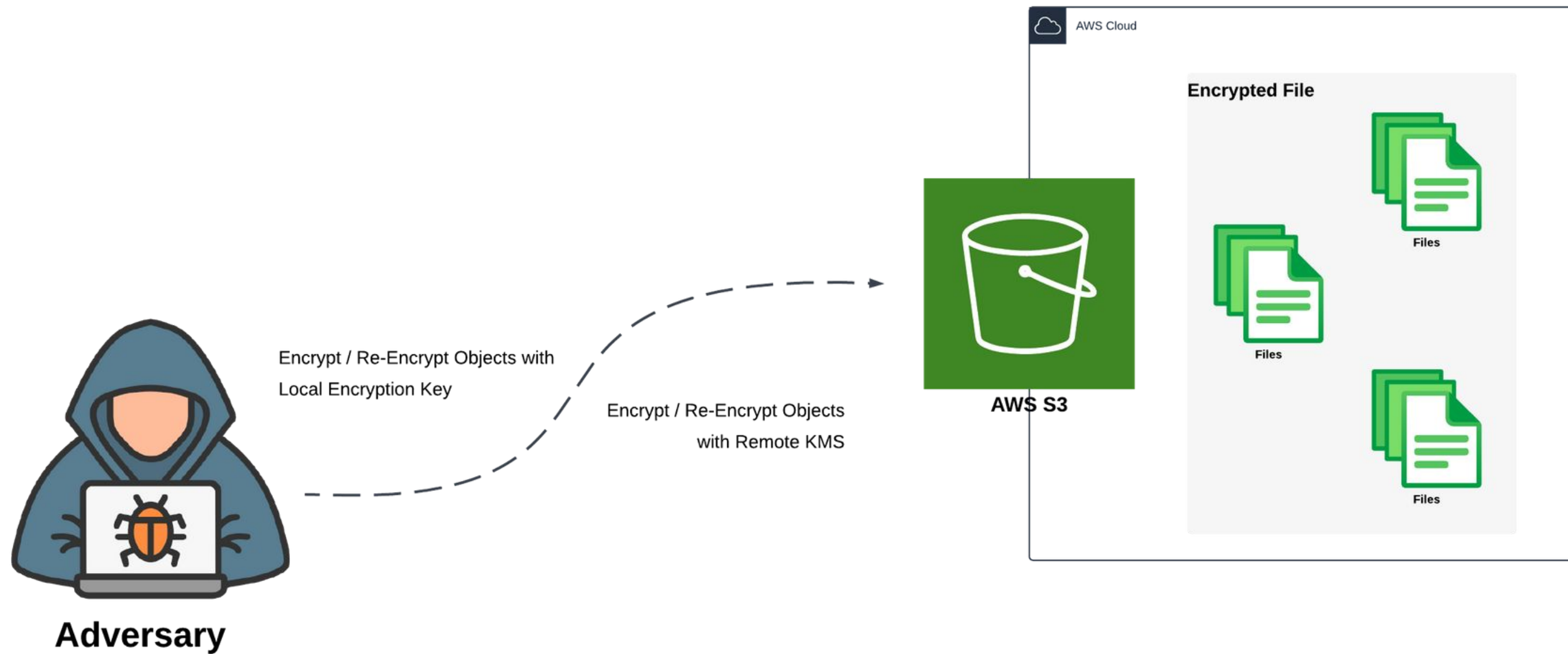
Resource Hijacking



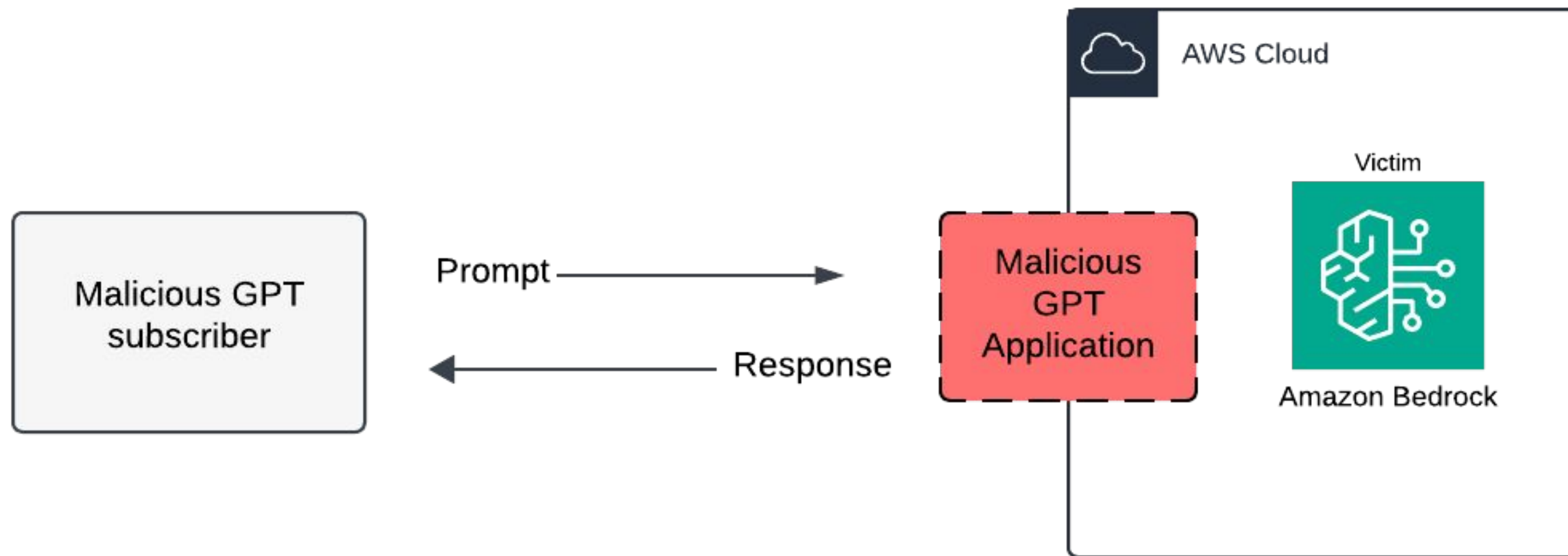
Data Destruction



Cloud-Specific Ransomware

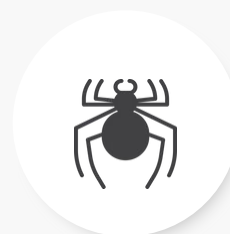


Hijacking victim AI infrastructure



APTs targeting cloud

As organizations move more services and applications to the cloud, adversaries have adapted their strategies to exploit the expanded attack surface. Threat actors now leverage the same cloud services as their targets.



**SCATTERED
SPIDER**



**COZY
BEAR**



**COSMIC
WOLF**

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement
5 techniques	5 techniques	7 techniques	5 techniques	13 techniques	11 techniques	14 techniques	5 techniques
Drive-by Compromise	Cloud Administration Command	Account Manipulation (5)	Abuse Elevation Control Mechanism (1)	Abuse Elevation Control Mechanism (1)	Brute Force (4)	Account Discovery (2)	Internal Spearphishing
Exploit Public-Facing Application	Command and Scripting Interpreter (1)	Create Account (1)	Account Manipulation (5)	Domain or Tenant Policy Modification (1)	Credentials from Password Stores (1)	Cloud Infrastructure Discovery	Remote Services (2)
Phishing (2)	Serverless Execution	Event Triggered Execution	Domain or Tenant Policy Modification (1)	Exploitation for Defense Evasion	Exploitation for Credential Access	Cloud Service Dashboard	Software Deployment Tools
Trusted Relationship	Software Deployment Tools	Implant Internal Image	Event Triggered Execution	Hide Artifacts (1)	Forge Web Credentials (2)	Cloud Service Discovery	Taint Shared Content
Valid Accounts (2)	User Execution (1)	Modify Authentication Process (3)	Valid Accounts (2)	Impair Defenses (3)	Modify Authentication Process (3)	Cloud Storage Object Discovery	Use Alternate Authentication Material (2)
		Office Application Startup (6)		Impersonation	Multi-Factor Authentication Request Generation	Log Enumeration	
		Valid Accounts (2)		Indicator Removal (1)	Network Sniffing	Network Service Discovery	
				Modify Authentication Process (3)	Steal Application Access Token	Password Policy Discovery	
				Modify Cloud Compute Infrastructure (5)	Steal or Forge Authentication Certificates	Permission Groups Discovery (1)	
				Modify Cloud Resource Hierarchy	Steal Web Session Cookie	Software Discovery (1)	
				Unused/Unsupported Cloud Regions	Unsecured Credentials (3)	System Information Discovery	
				Use Alternate Authentication Material (2)			
				Valid Accounts (2)			

Mitre Cloud Matrix

The MITRE Cloud Matrix is a specialized framework within the MITRE ATT&CK knowledge base, focusing on cloud-specific tactics, techniques, and procedures (TTPs) used by adversaries. It maps out how attackers exploit cloud environments — such as AWS, Azure, and GCP — across key stages like initial access, privilege escalation, and data exfiltration. This matrix helps security teams understand, detect, and respond to cloud-based threats more effectively.

Investigating Azure Blob Deletion Activity Using Key Vault Secret

As part of the security team of Secure-corp, the participant is tasked with identifying suspicious activities like unauthorized deletion of blob through unusual access to the KeyVault secret.



Solve to Win BTF

Thank You

For Professional Red Team / Blue Team / Purple Team / Cloud Cyber Range labs / Trainings, please contact
support@cyberwarfare.live

To know more about our offerings, please visit: <https://cyberwarfare.live>

[www.cyberwarfare.live](https://cyberwarfare.live)