CWL
CyberWarFare Labs

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

CWL
CyberWarFare Labs

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.

CWL
CyberWarFare Labs

Table of Content

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 Exfilteration

6 Impact

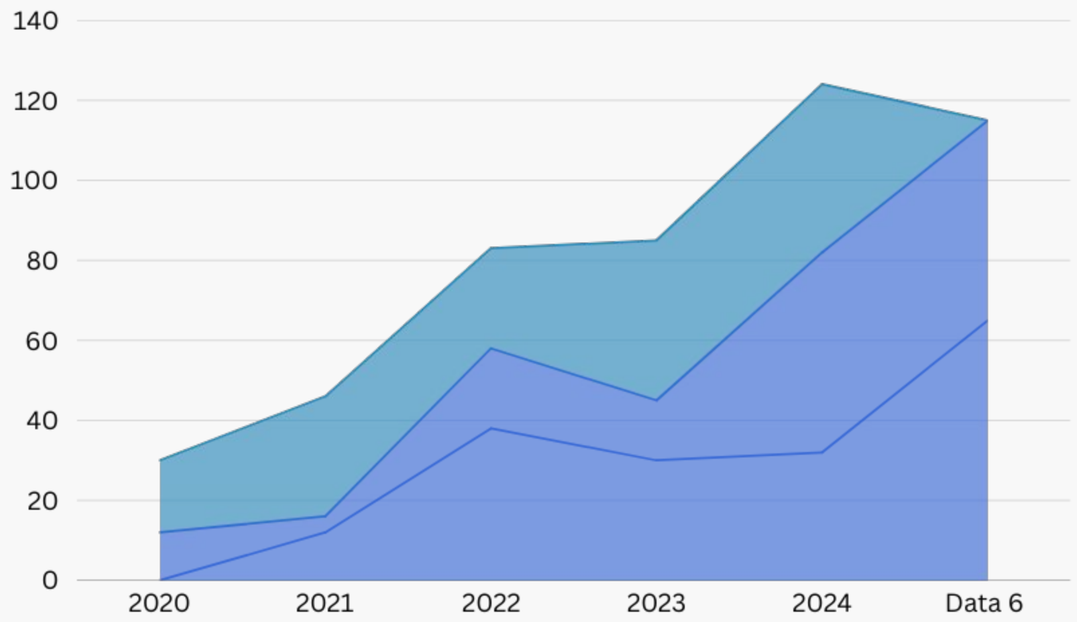
- Resource hijacking
- Data Encryption/destruction

Cloud breaches statistics

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

27% of organizations experienced a public cloud security incident

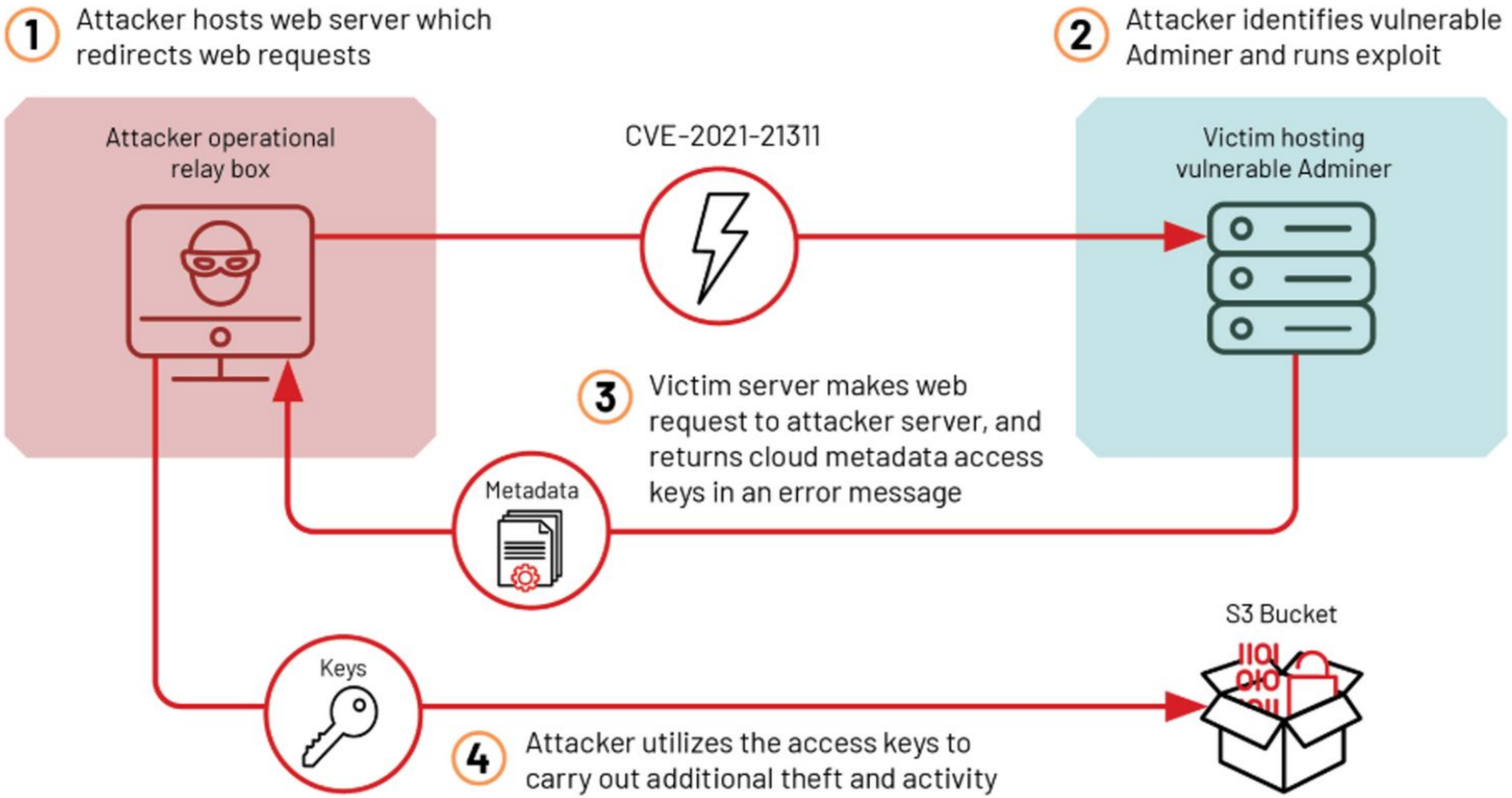
62% of organizations reported they were either somewhat or highly likely to experience a cloud data breach in the next year.



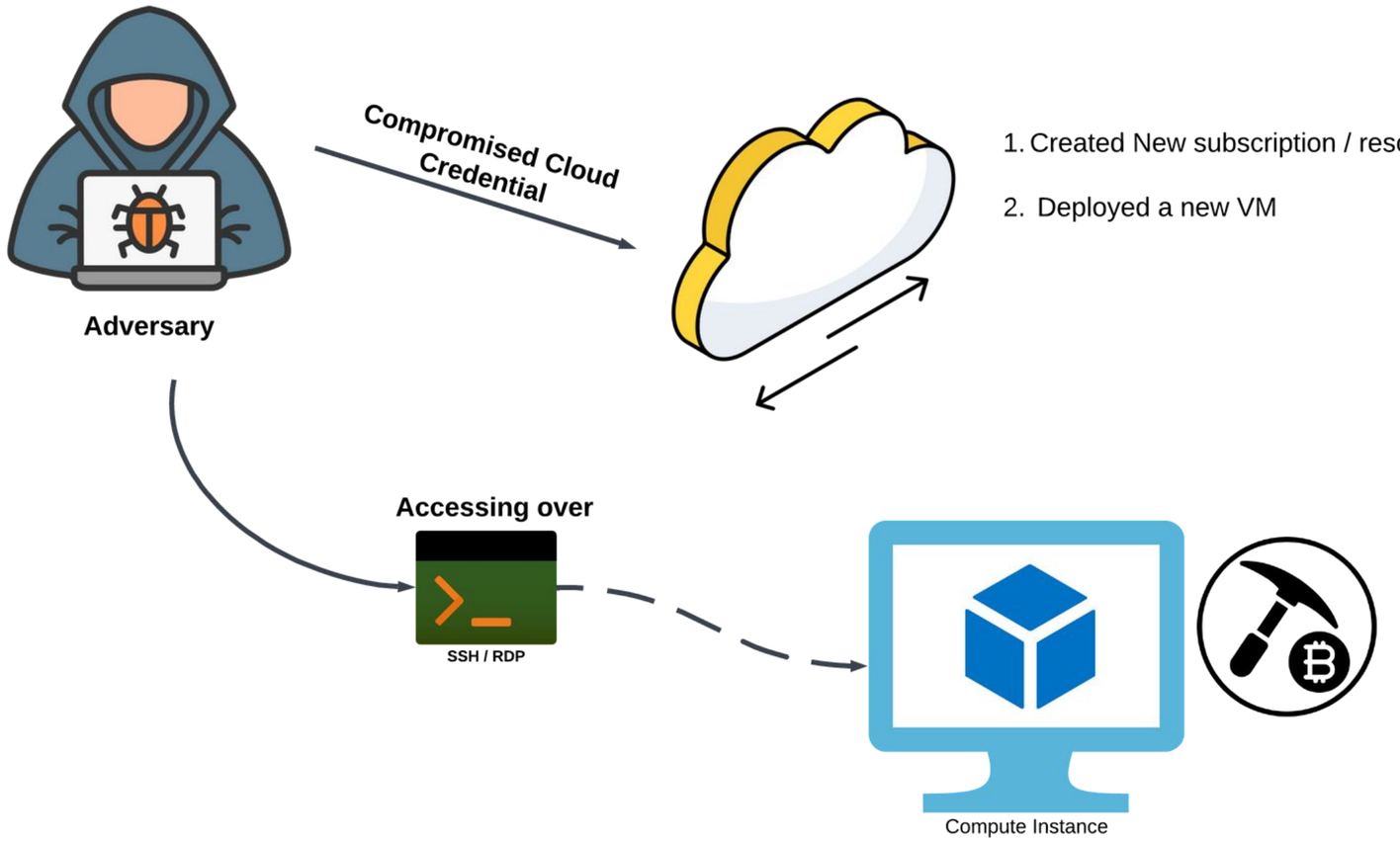
Emerging Cloud Security Threats

- IMDS Credential Access
- Resource Hijacking
- Cloud-Specific Ransomware
- Data Destruction
- Hijacking GenAI infrastructure

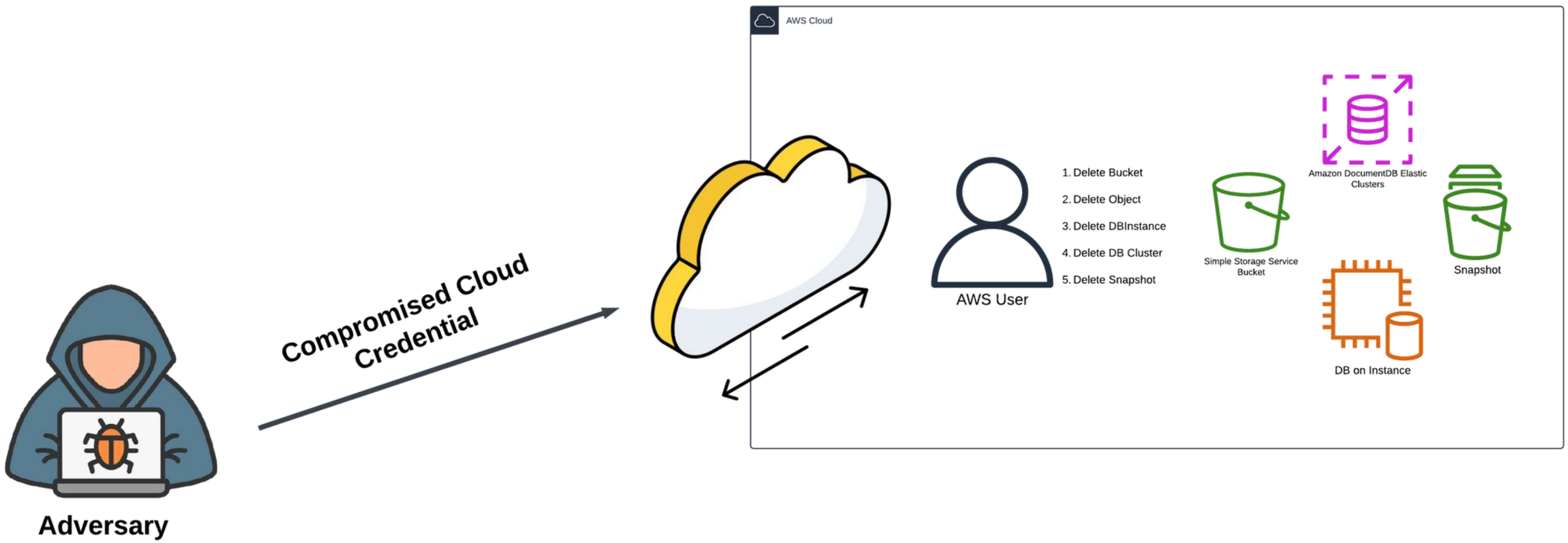
IMDS Credential Access



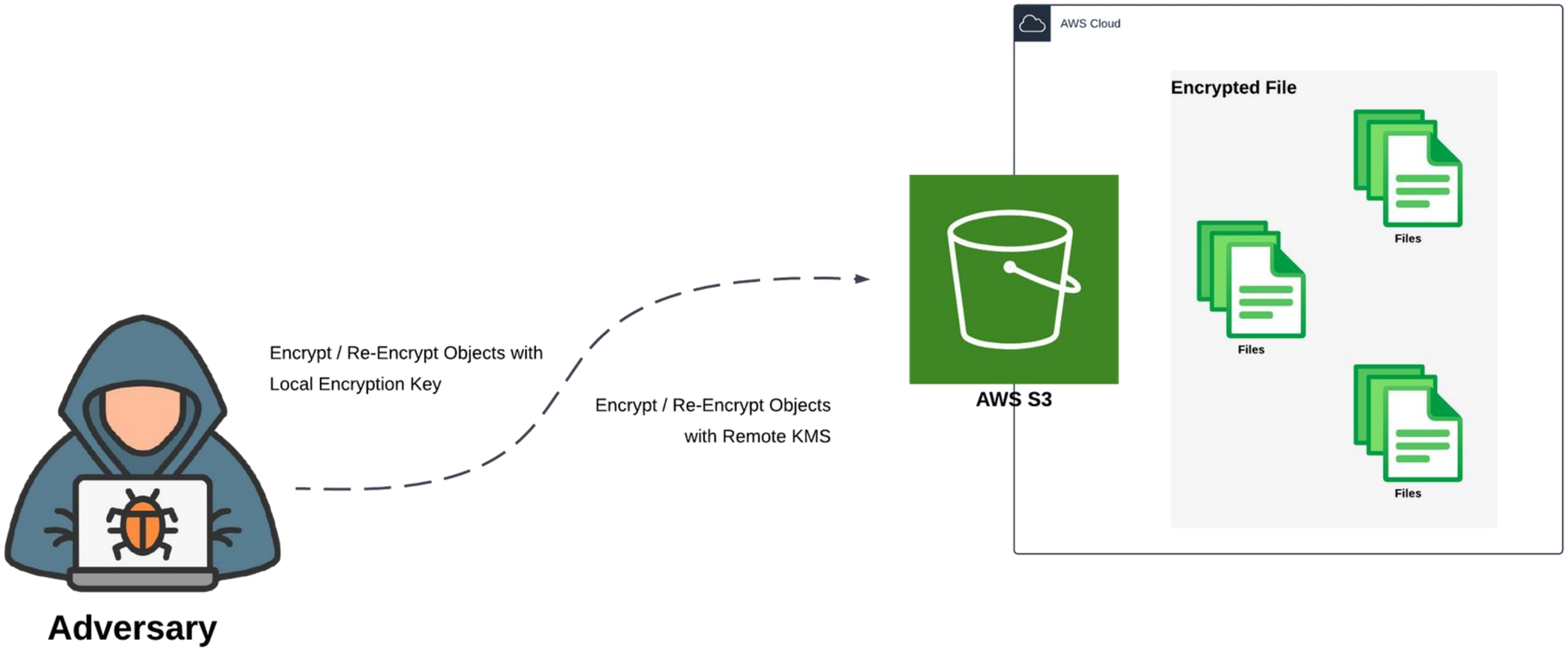
Resource Hijacking



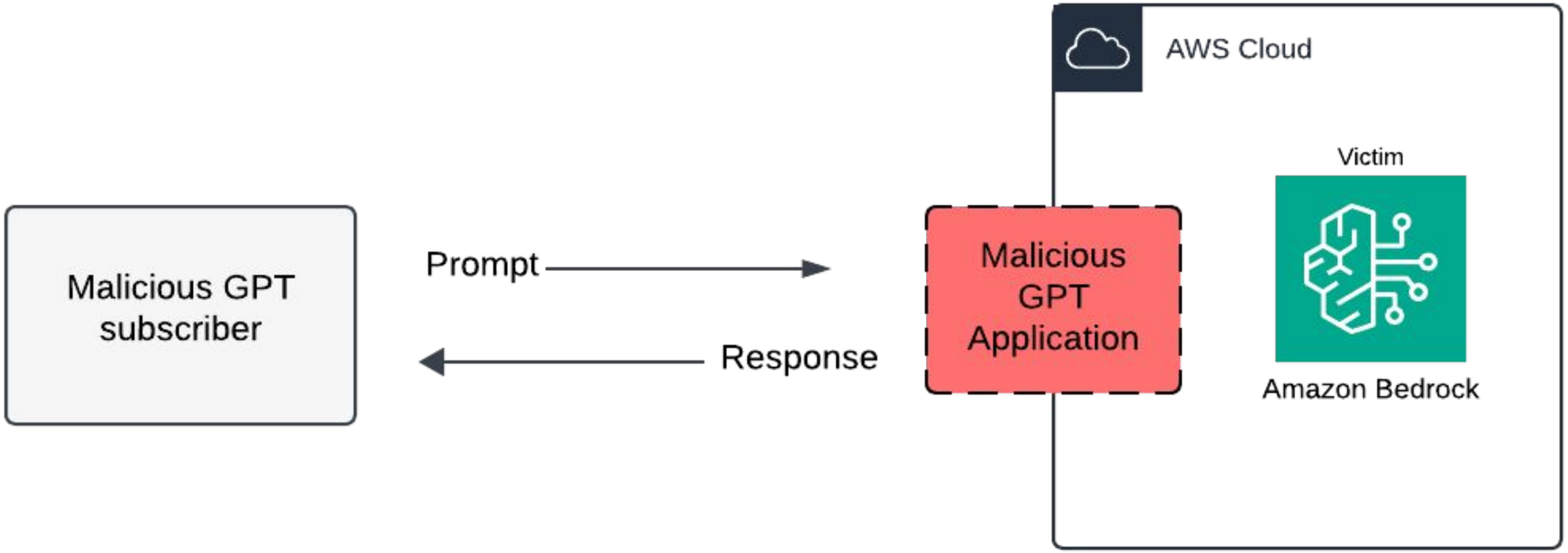
Data Destruction



Cloud-Specific Ransomware

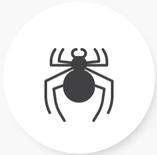


Hijacking victim AI infrastructure



APTs targeting cloud

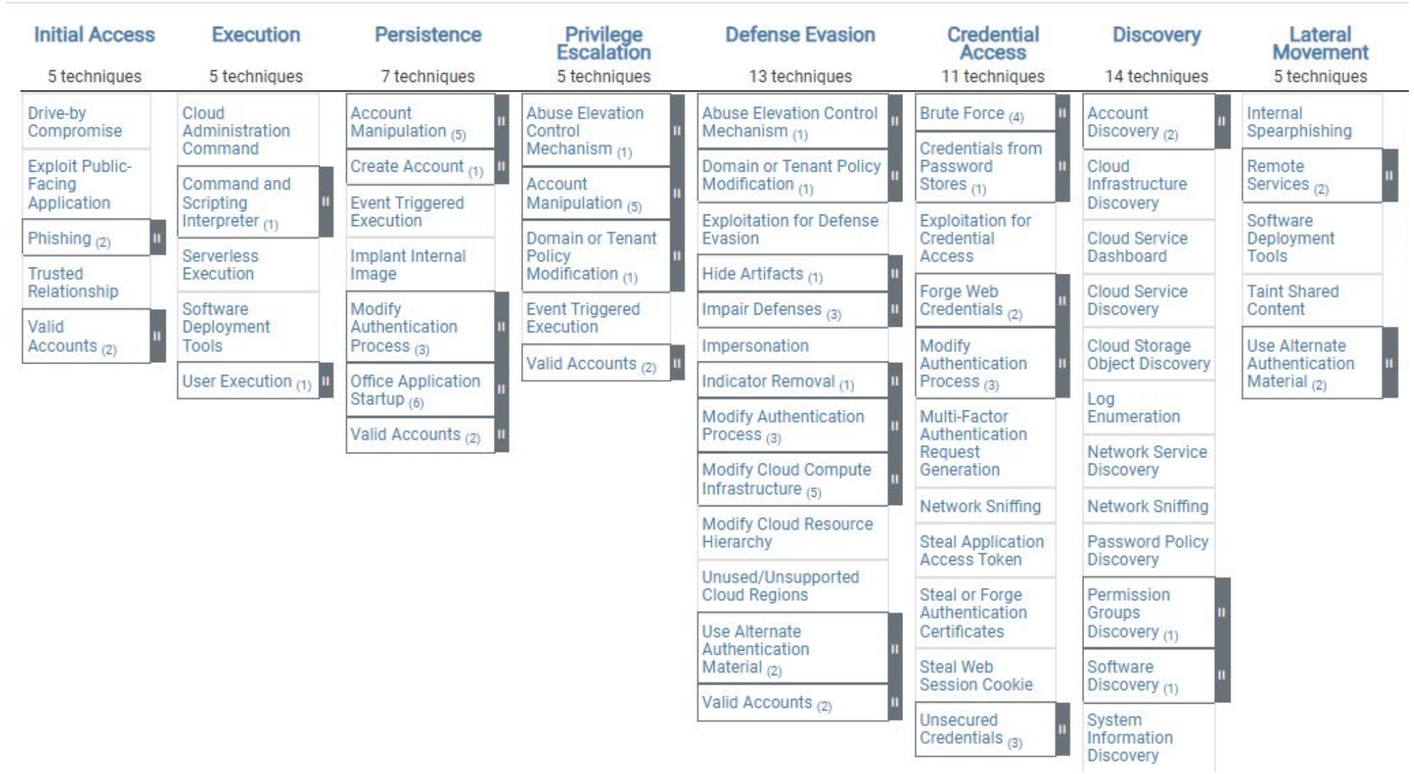
As organizations move more services and applications to the cloud, adversaries have adapted their strategies to exploit the expanded attack surface. Threat actors now leverage the same cloud services as their targets.



SCATTERED SPIDER

COZY BEAR

COSMIC WOLF



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