



MITRE ATT&CK in Amazon Web Services (AWS):
A defender's cheat sheet

Bottom line:

Chasing down AWS GuardDuty alerts and combing through CloudTrail logs can be tough if you don't know what to look for (or even if you do).

Knowing which API calls are associated with different attack tactics isn't intuitive – which is why we created this handy cheat sheet to help you while you're investigating incidents in AWS.

A helpful way to map MITRE ATT&CK tactics to AWS API calls

This guide contains a breakdown of the tactics we see attackers use most often during attacks in AWS.

In order to give you a jump start on investigations in your own AWS environment, we've mapped the AWS services in which these tactics often originate (thanks, crafty attackers) along with the API calls the attackers make to execute on said techniques.

As a bonus, we're throwing in some of our own tips and tricks that you can use when you're investigating an incident in AWS that's related to any of these attack tactics.

How to use this cheat sheet

This cheat sheet is intended to be a resource to help answer investigative questions during AWS alert triage, investigations and incident response. You can use it to quickly identify potential attacks in AWS and map them to MITRE ATT&CK tactics.

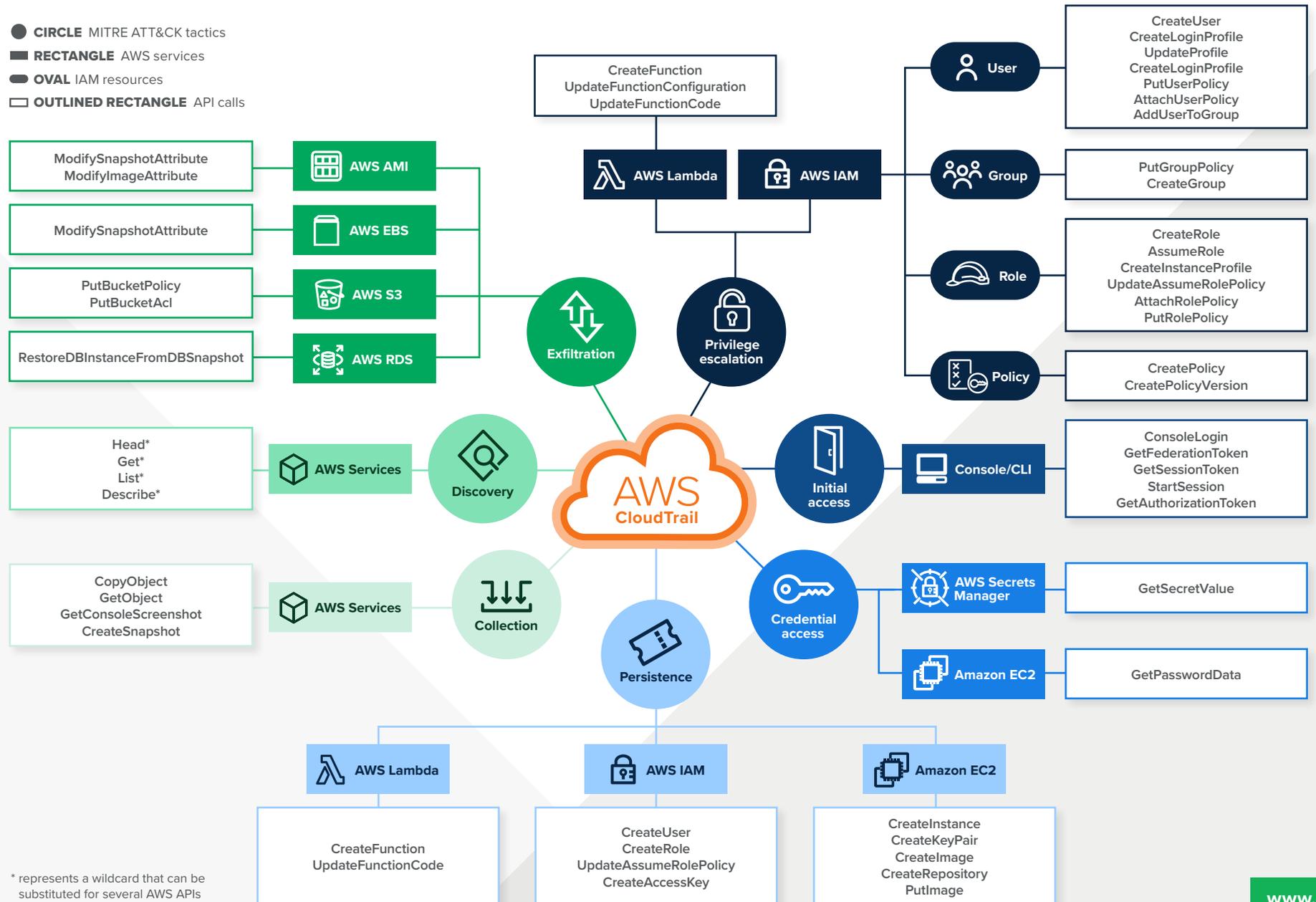
Depending on which phase of an attack you're investigating, you can also use it to identify other potential attack paths and MITRE ATT&CK tactics the attacker might have used. This'll help you see the bigger picture and identify risky activity and behaviors that could indicate you're compromised and require remediation.

For example, if you see suspected credential access, you can investigate to check how that principal authenticated to AWS, if they've assumed any other roles and if there are any other suspicious API calls that could represent if this were an attacker. Some other tactics that an attacker could have executed prior to credential access are discovery, persistence and privilege escalation.

AWS mind map for investigations and incidents

MITRE ATT&CK tactics

- **CIRCLE** MITRE ATT&CK tactics
- **RECTANGLE** AWS services
- **OVAL** IAM resources
- **OUTLINED RECTANGLE** API calls



* represents a wildcard that can be substituted for several AWS APIs

A closer look at tactics, techniques and API calls

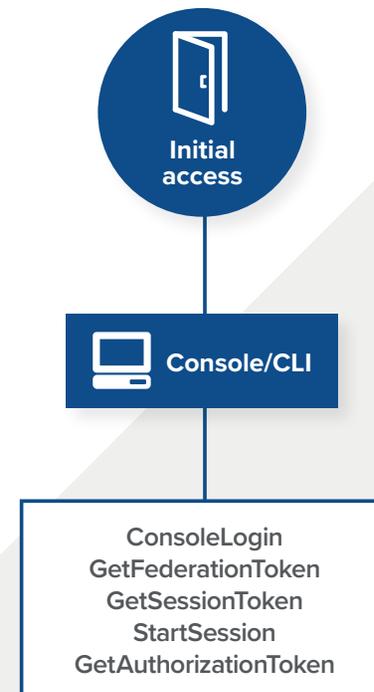


To help you get a better sense of how we think about our investigations in AWS, let's take a closer look at the tactics, techniques and associated API calls attackers might use.

MITRE ATT&CK tactic:

Initial access

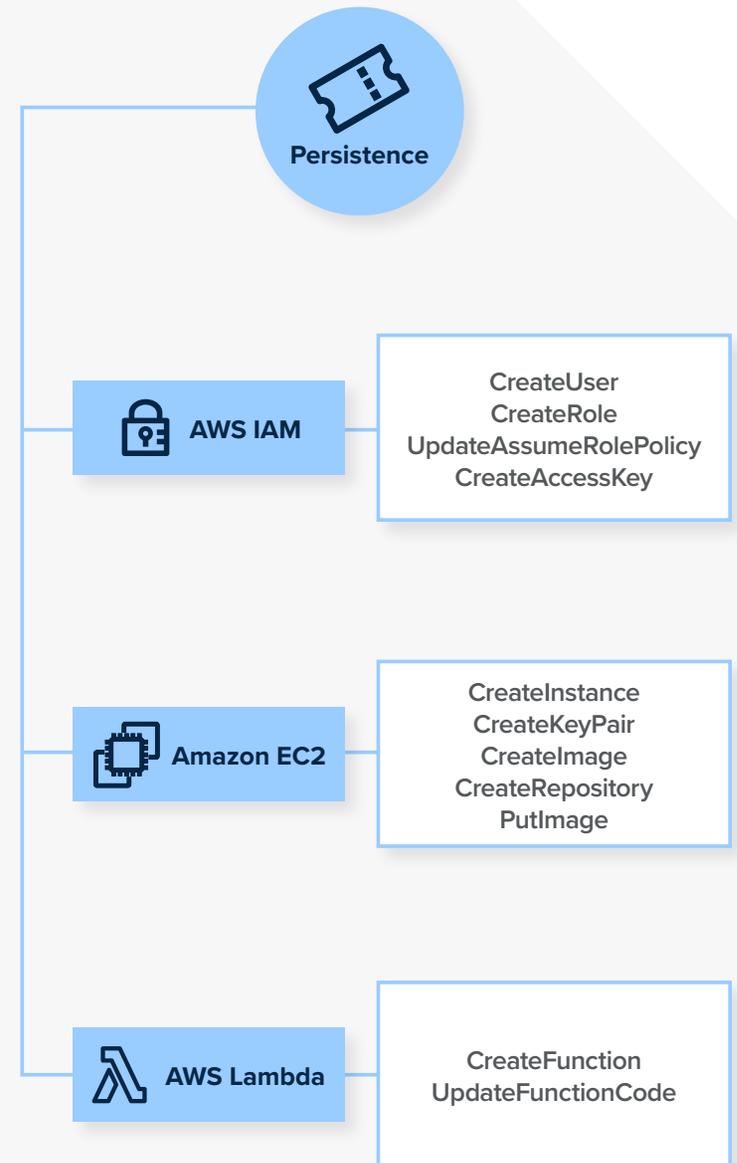
- **Why attackers do it:** To gain access to your AWS environment.
- **How attackers execute it:** AWS console or command-line interface.
- **Look for these API calls:** ConsoleLogin, GetFederationToken, GetSessionToken, StartSession and GetAuthorizationToken.
- **Investigation tips and tricks:** Review the source of authentication, user-agent strings and the credentials used to access the AWS environment. Investigate the authenticating principal, geo-impossible authentications, suspicious IP addresses and anomalous authentication behavior to identify whether this is legitimate access.



MITRE ATT&CK tactic:

Persistence

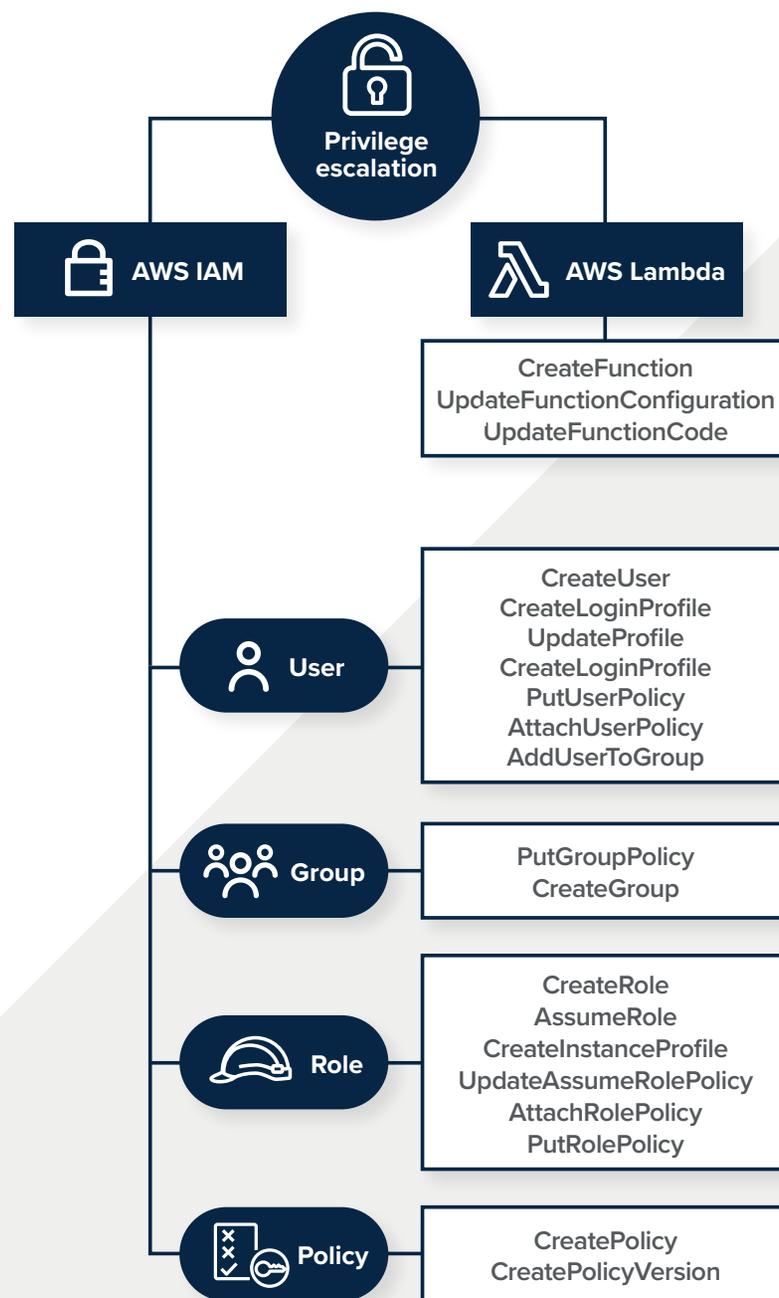
- **Why attackers do it:** To maintain access to your AWS environment across any interruptions.
- **How attackers execute it:** Identity and Access Management (IAM), AWS Lambda and Amazon Elastic Compute Cloud (EC2).
- **Look for these API calls:** CreateFunction, UpdateFunctionCode, CreateUser, CreateRole, UpdateAssumeRolePolicy, CreateAccessKey, CreateInstance, CreateKeyPair, CreateImage, CreateRepository and PutImage.
- **Investigation tips and tricks:** Look out for new or updated IAM resources, Amazon EC2 resources or backdoor Lambda functions. Persistence in these services is intended to provide the attacker a means to re-enter the AWS environment. Attackers may also rotate access keys for compromised accounts.



MITRE ATT&CK tactic:

Privilege escalation

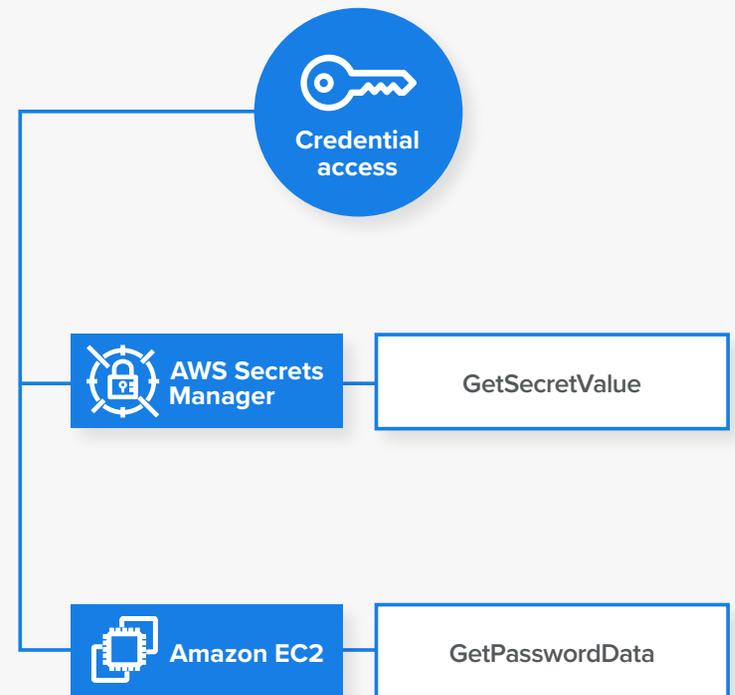
- **Why attackers do it:** To gain higher-level permissions within your AWS environment and complete their objective(s). Elevated permissions are typically required to establish persistence, access credentials and perform collection and exfiltration.
- **How attackers execute it:** AWS IAM and AWS Lambda.
- **Look for these API calls:** CreateFunction, UpdateFunctionConfiguration, UpdateFunctionCode, CreatePolicy, CreatePolicyVersion, CreateRole, AssumeRole, CreateInstanceProfile, UpdateAssumeRolePolicy, AttachRolePolicy and PutRolePolicy.
- **Investigation tips and tricks:** Look out for IAM groups, roles, policies or users being created or modified after unauthorized access. The attacker may attach IAM resources to a compromised or newly created user to inherit elevated permissions. Lambda functions may also be used to automate the abuse of IAM resources to gain these permissions.



MITRE ATT&CK tactic:

Credential access

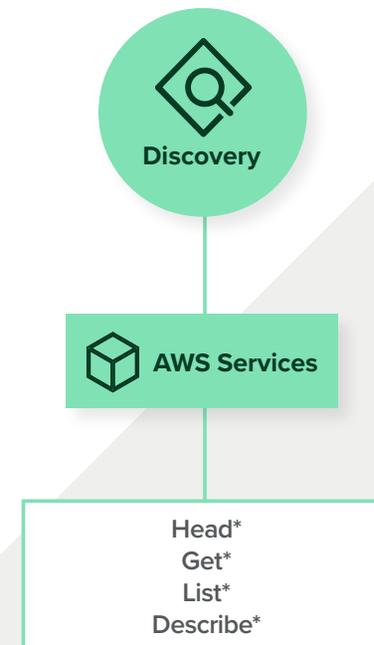
- **Why attackers do it:** To access and acquire credentials in the AWS environment. Stolen credentials may allow attackers to gain access to different AWS resources, settings and permissions.
- **How attackers usually execute it:** Amazon EC2 and AWS Secrets manager.
- **Look for these API calls:** GetPasswordData and GetSecretValue.
- **Investigation tips and tricks:** Review the principal authentication details, source of activity and other API calls performed by the Amazon Resource Name (ARN) to see if this behavior is abnormal. An attacker will likely have performed a series of other events prior to attempting to access credentials.



MITRE ATT&CK tactic:

Discovery

- **Why attackers do it:** To discover and enumerate sensitive information about the AWS environment.
- **How attackers usually execute it:** AWS services.
- **Look for these API calls:** Majority of APIs that begin with Get*, List*, Head* and Describe*.
- **Investigation tips and tricks:** Automated reconnaissance typically occurs in bursts and can be noisy in CloudTrail logs. Investigate the principal and the ARN to see if these API calls are inline with expected behavior. A time series of API calls can be helpful when determining if these API calls are expected behavior.



* represents a wildcard that can be substituted for several AWS APIs

MITRE ATT&CK tactic:

Collection

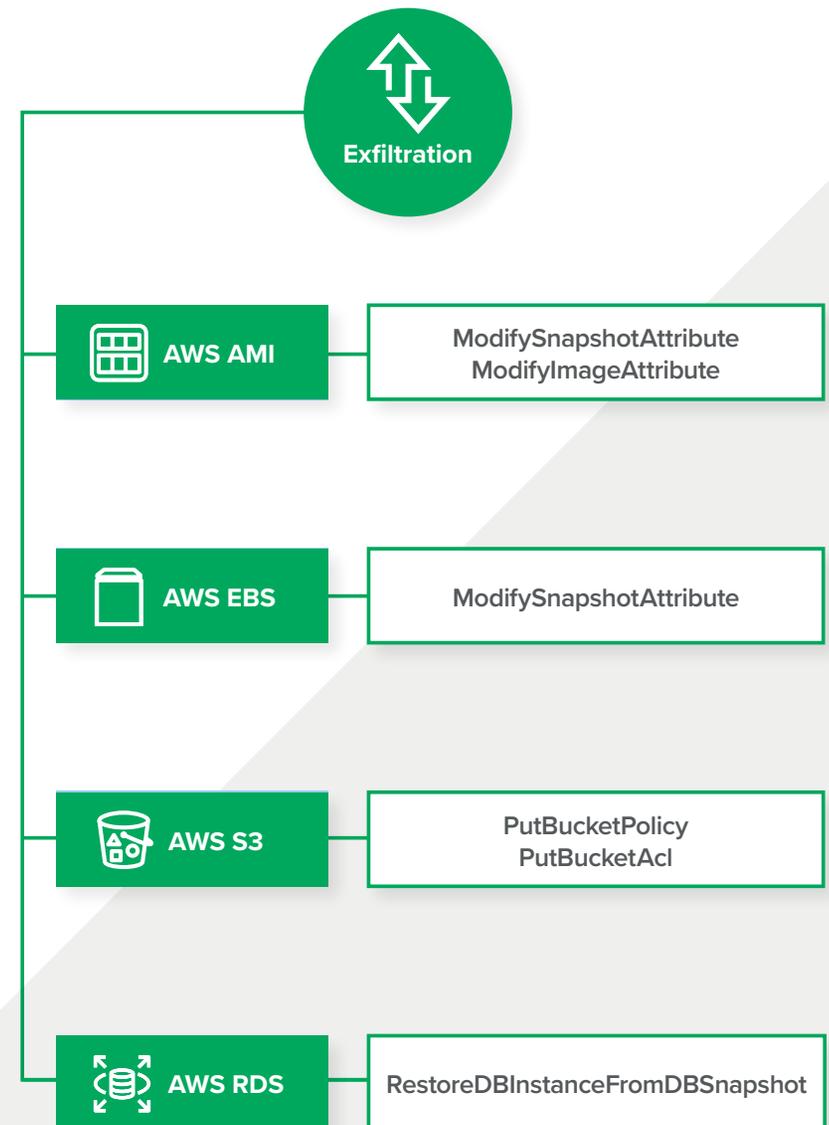
- **Why attackers do it:** To collect sensitive data from AWS resources and services. Attackers typically exfiltrate collected data to their own infrastructure.
- **How attackers usually execute it:** Amazon EC2 and Amazon Simple Storage Service (S3).
- **Look for these API calls:** CopyObject, GetObject, GetConsoleScreenshot and CreateSnapshot.
- **Investigation tips and tricks:** Look out for any data collection from S3 buckets and EC2 instances. Investigate the principal to see where they authenticated from and if they typically interact with these AWS services to collect sensitive information. Historical CloudTrail logs for these resources and API calls may also provide insight into whether or not this is expected activity in the environment.



MITRE ATT&CK tactic:

Exfiltration

- **Why attackers do it:** To remove sensitive information and data from the AWS environment to attacker-controlled infrastructure.
- **How attackers usually execute it:** Amazon Machine Image (AMI), Amazon Elastic Block Store (EBS), Amazon S3 and Amazon Relational Database Service (RDS).
- **Look for these API calls:** ModifySnapshotAttribute, ModifyImageAttribute, ModifySnapshotAttribute, PutBucketPolicy, PutBucketAcl, RestoreDBInstanceFromDBSnapshot.
- **Investigation tips and tricks:** Look out for any abnormal changes to AWS AMI, EBS, S3 and RDS services that would allow the attacker to copy, move or make the resources publicly available – especially if there isn't a known business need. If you spot suspected exfiltration, investigate the ARN and principal's previous API calls, source and method of authentication along with user-agent string to see if this is inline with normal behavior.



(this is the last page)



Our SOC-as-a-service capability offers 24x7 security monitoring and response for cloud, hybrid and on-premises environments. We use the security signals our customers already own so organizations can get more value from their existing security investments. We connect to customer tech remotely through APIs, not agents, so our SOC can start monitoring a customer's environment in a matter of hours, letting their internal teams get back to focusing on the most strategic security priorities that are unique to their business. Learn more at www.expel.io.