

Técnicas de prevenção de ataques e resposta a incidentes em ambientes AWS

Esta apresentação tem por objetivo apresentar orientações para aumentar o nível de segurança dos workloads, a partir de análises de estudos de caso de incidentes reais e o que poderia ter sido feito para evitá-los



Profile

- 24 anos na gestão de times de TI e Segurança da Informação
- Graduação em Ciência da computação com especialização redes e Cloud
- MBA Gestão estratégica de TI pela FGV





Agenda

- Introdução
- Modelo de responsabilidade compartilhada
- Estatísticas de ameaças
- Estudos de caso
 - Medidas de prevenção
 - Respostas a incidentes
- Conclusão

Infraestrutura global



- 245 países
- 32 regiões
- 102 AZs
- +300 serviços

Introdução



- Fornecedores despreparados
- Treinamentos sem foco em segurança
 - Não façam isso em casa!!
- Grande poder computacional em mãos inábeis
 - Prejuízos exponenciais

- É de suma importância selecionar bem os fornecedores e analisar o tipo de acesso que está sendo solicitados pelos menos, para evitar exposição desnecessária
- Muitos treinamentos de Cloud, são realizados através a utilização de contas administrativas e sem o uso de qualquer configuração de segurança, utilizando como pretexto serem apenas para “fins didáticos”. Ainda que usado por um breve espaço de tempo, isso pode expor a conta do usuário a invasões.
Considero de suma importância, desde o aprendizado inicial, utilizar o princípio de segurança by design.
- A AWS disponibiliza vários treinamentos de segurança gratuitos através do Skill Builder (<https://explore.skillbuilder.aws/learn/signin>)



Modelo de responsabilidade compartilhada

Modelo de Responsabilidade compartilhada



É muito importante que o usuário tenha conhecimento de suas responsabilidades para a gestão de sua conta na AWS e os respectivos workloads.

Para isso a AWS criou o modelo de responsabilidade compartilhada, um documento que define de forma clara e objetiva o que compete a cada uma das partes envolvidas

<https://aws.amazon.com/pt/compliance/shared-responsibility-model/>



Estatísticas de ameaças

Ameaças

- AWS sofre um quadrilhão de ataques por mês
- 84,1% concedem acessos privilegiados de IAM em imposição de MFA
- 68% contas de terceiros tem acessos administrativos
- 59,4% não aplicam controles básicos de segurança
- 36% das organizações possuem pelo menos um bucket público
 - Um bucket público leva em média de 7 a 13 horas ser acessado por hackers
- 17,4% executam workloads com vulnerabilidades expostos a Internet

Fonte: AWS, Zscaler, DataDog, Wiz

<https://www.zscaler.com/blogs/security-research/2022-cloud-insecurity-report>
<https://www.datadoghq.com/state-of-aws-security/>

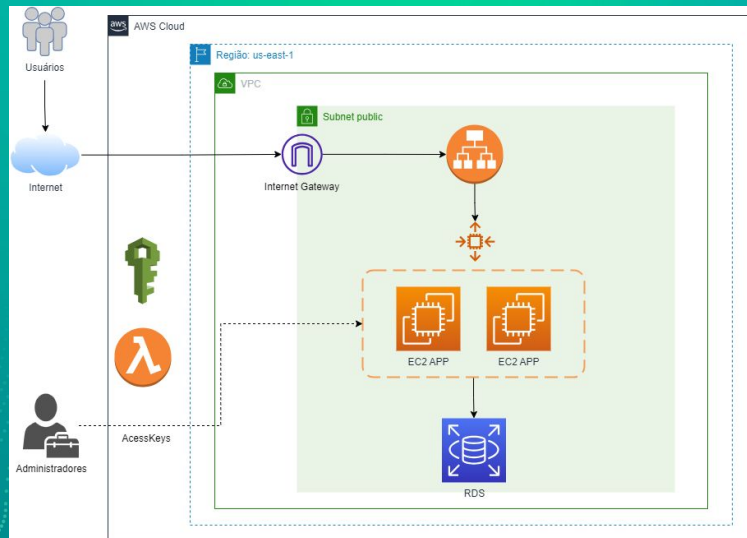
From exposure to discovery: how fast do hackers find open buckets?



Estudios de caso

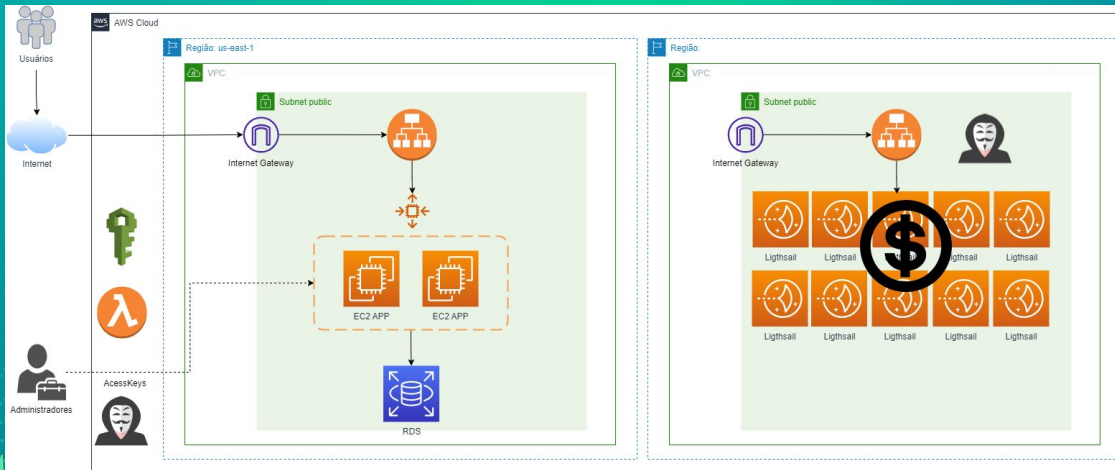
Invasão da Startup

Invasão da Startup



- Este diagrama representa a estrutura inicial criada pela Startup, apresentando várias falhas de segurança
 - Todos os serviços foram alocados em uma subnet pública, ficando expostos a Internet e muito mais vulneráveis a ataques
 - Foram utilizadas configurações permissivas para os security groups e network acls
 - Nenhum serviço de segurança adicional foi configurado
 - A administração do ambiente era realizada através de acesso programático utilizando AccessKeys/SecretKeys

Invasão da Startup




- A invasão da estrutura foi realizada através do roubo da AccessKey configurada em um computador utilizado pelo administrador, após ser infectado por vírus
- O invasor criou uma estrutura paralela em uma região não utilizada pelo usuário, utilizando instâncias muito robustas aumento bruscamente o custo de serviços utilizados
- Neste tipo de ataque, é muito comum que o invasor não interfira no funcionamento do workload mantido pelo usuário, para retardar ao máximo a identificação do incidente

Resposta a incidente

- Identificar
- Conter
- Coletar evidências
- Restaurar/Reparar
- Aplicar ajustes

- Um plano de resposta a incidentes eficiente, deve ser desenvolvido, homologado e testado, sob medida para para organização
- Serão apresentadas as principais etapas que são comumente encontradas para este tipo de documento

Identificar origem



Report Information

Version: 3.4.1

Parameters used: aws --profile auditoria

Date: 2023-05-09T20:24:51.512Z

AWS Assessment Summary

AWS Account: 44355617628

AWS-CLI Profile: auditoria

Audited Regions: All Regions

AWS Credentials

User Id: AIDAWC...

Caller Identity ARN: arn:aws:iam::44355617628:user/auditoria

Assessment Overview

Total Findings: 1434

Passed: 964

Failed: 470

Total Resources: 223

Filters (4) Show 100 entries

Search:

Status	Severity	Service Name	Region	Check ID	Check Title	Resource ID	Resource Tags	Status Extended	Risk	Recommendation	Compliance
FAIL	medium	ec2	us-east-1	ec2_ebs_snapshots_encrypted	Check if EBS snapshots are encrypted.	snap-026e6d15583627e4	*Name=LAB-SEC	EBS Snapshot snap-026e6d15583627e4 is unencrypted.	Data encryption at rest preven read more...	Encrypt all EBS Snapshot and E read more...	<ENS-RD2022: mps.i2.aws.elb, read more...
FAIL	medium	ec2	us-east-1	ec2_ebs_snapshots_encrypted	Check if EBS snapshots are encrypted.	snap-0cd37b4ba6209ad3f		EBS Snapshot snap-0cd37b4ba6209ad3f is unencrypted.	Data encryption at rest preven read more...	Encrypt all EBS Snapshot and E read more...	<ENS-RD2022: mps.i2.aws.elb, read more...
FAIL	medium	ec2	us-east-1	ec2_ebs_snapshots_encrypted	Check if EBS snapshots are encrypted.	snap-0dd12e04b5f770923		EBS Snapshot snap-0dd12e04b5f770923 is unencrypted.	Data encryption at rest preven read more...	Encrypt all EBS Snapshot and E read more...	<ENS-RD2022: mps.i2.aws.elb, read more...
FAIL	medium	ec2	us-east-1	ec2_ebs_snapshots_encrypted	Check if EBS snapshots are encrypted.	snap-056f1fe2ebd00c91e		EBS Snapshot snap-056f1fe2ebd00c91e is unencrypted.	Data encryption at rest preven read more...	Encrypt all EBS Snapshot and E read more...	<ENS-RD2022: mps.i2.aws.elb, read more...

Showing 1 to 4 of 4 entries (filtered from 1,438 total entries)

Previous

1

Next

Showing 1 to 4 of 4 entries (filtered from 1,438 total entries)

Previous 1 Next

- Para identificar a origem de um ataque, é de suma importância ter uma inventario devidamente documentado atualizado, de todos os recursos utilizados na conta
- Através do serviço AWS Config, é possível realizar o inventário restrito a região em uso. Levando em conta que atualmente a AWS disponibiliza 32 regiões, é recomendado utilizar outros serviços que possam executar a tarefa de forma mais eficiente
- O Prowler Cloud é um dos serviços que podem atender esta necessidade do usuário:
 - Disponível na versão Community e Enterprise, permite realizar a análise da conta e gerar um relatório de todos os recursos em uso
 - A ferramenta também gera uma relação de todas as vulnerabilidades identificadas, agrupadas por nível de criticidade, podendo ser utilizada como base para a aplicação de ajustes e correções
 - <https://github.com/prowler-cloud/prowler>

Identificar origem

Event history (50+) Info

Event history shows you the last 90 days of management events.

Lookup attributes

AWS access key

<input type="checkbox"/>	Event name	Event time	User name	AWS access key
<input type="checkbox"/>	DescribeLoadBalancers	May 05, 2023, 16:22:16 (UTC-03:00)	terraform	ASIAWOR[REDACTED]
<input type="checkbox"/>	DescribeInstances	May 05, 2023, 16:22:15 (UTC-03:00)	terraform	ASIAWOR[REDACTED]
<input type="checkbox"/>	DescribeAddresses	May 05, 2023, 16:22:15 (UTC-03:00)	terraform	ASIAWOR[REDACTED]
<input type="checkbox"/>	DescribeLoadBalancers	May 05, 2023, 16:22:15 (UTC-03:00)	terraform	ASIAWOR[REDACTED]
<input type="checkbox"/>	DescribeInstanceStatus	May 05, 2023, 16:22:15 (UTC-03:00)	terraform	ASIAWOR[REDACTED]
<input type="checkbox"/>	DescribeHosts	May 05, 2023, 16:22:15 (UTC-03:00)	terraform	ASIAWOR[REDACTED]

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAWOR6D[REDACTED]",
    "arn": "arn:aws:iam::[REDACTED]:user/terraform",
    "accountId": "443[REDACTED]9",
    "accessKeyId": "ASIAW[REDACTED]I",
    "userName": "terraform",
    "sessionContext": {
      "sessionIssuer": {},
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2023-05-05T18:01:11Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2023-05-05T18:02:01Z",
  "eventSource": "autoscaling.amazonaws.com",
  "eventName": "UpdateAutoScalingGroup",
  "awsRegion": "us-east-2",
  "sourceIPAddress": "186.210.76.114",
  "userAgent": "AWS Internal",
  "requestParameters": {
    "maxSize": 1,
    "minSize": 1,
    "desiredCapacity": 1,
    "autoScalingGroupName": "as-[REDACTED]"
  }
}
```

- O Event History gerado pelo Cloud Trail, também pode ser utilizado para rastrear os serviços criados pelo atacantes e quais contas foram utilizadas para isso
- Por padrão a AWS mantém o log das chamadas de API realizadas no control plane por um período de 90 dias
- Caso o usuário precisar armazenar os registros por mais tempo ou ativar os registros do data plane, é necessário realizar intervenção manual

Contenção

- Bloquear acesso de todas AccessKey em uso
 - Ativar *condictions* para restringir o acesso (IP de origem)
 - Realizar rotacionamento gradativo após os devidos ajustes
- Alterar a senha de todos os usuários ativos
 - Ativar MFA
- Gerar novo par de chaves de acesso
- Desativar scripts Lambda

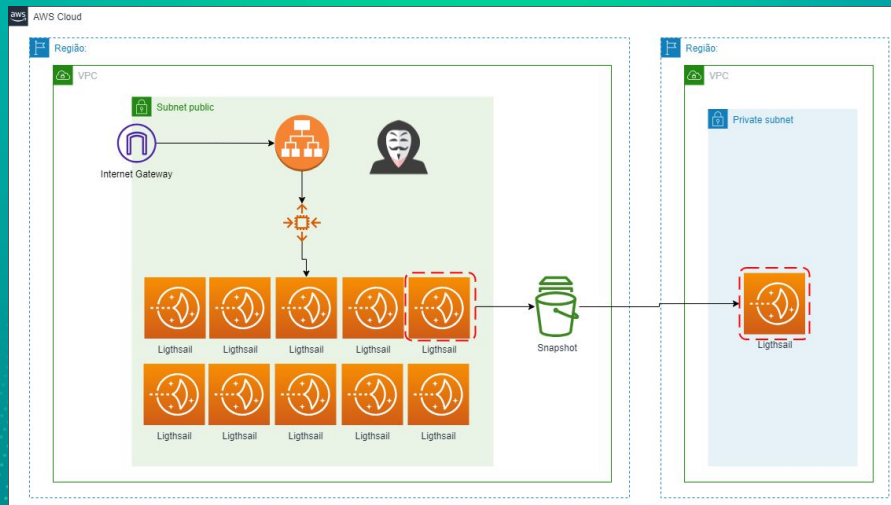
- Após identificar a origem do ataque, é necessário bloquear o acesso do atacante o mais breve possível

Coletar evidências

- Gerar cópia do histórico do CloudTrail em um bucket protegido
- Preservar instância

- Uma vez que a contenção do acesso tenha sido concluída, é necessário coletar e armazenar evidências do ataque em um local devidamente protegido para posterior análise forense, solicitar estorno de cobrança indevida à AWS e comunicar autoridades para e organizações reguladoras sobre o ocorrido
- É de suma importância criar uma cópia do histórico do Cloud Trail em um bucket criptografado e desativar o acesso a exclusão de conteúdo

Coletar evidências



- Para preservar o conteúdo de uma instância comprometida, as seguintes ações devem ser executadas:
 - Ativar a proteção contra exclusão automática
 - Remover a instâncias do grupo de AutoScaling
 - Configurar um security group bloqueando qualquer tipo de acesso
 - Gerar um snapshot criptografado do disco para posterior restauração em um ambiente controlado para análise do conteúdo

Reparar/Restaurar

- Excluir/desativar recursos e serviços utilizados pelo atacante
- Restaurar AMIs íntegras
- Restaurar cópias de segurança:
 - Aplicações
 - Bases de dados
- Realizar monitoramento e auditoria do ambiente

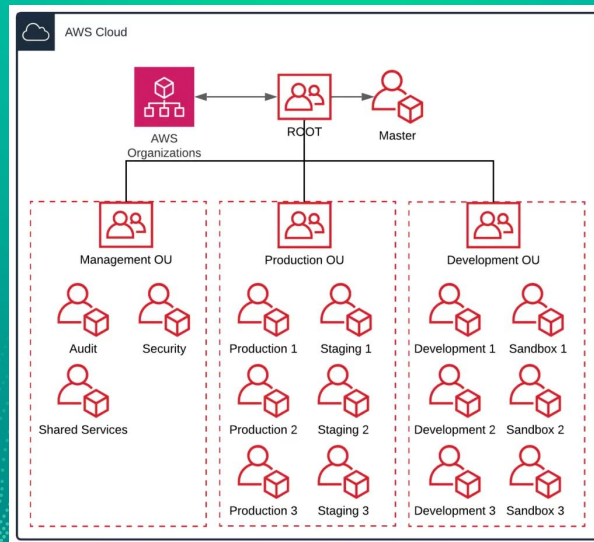
- Após a coleta de evidências, deve ser iniciada a reparação e restauração do ambiente
- Mais uma vez, é de suma importância contar com um inventário atualizado, para identificação de todos os recursos criados pelo invasor e providenciar sua exclusão

Aplicar ajustes

- Analisar evidências coletadas
- Desativar contas não utilizadas
 - Excluir AccessKeys
- Princípio de privilégio mínimo
- Utilizar Roles (devidamente parametrizadas) ao invés de AccessKey

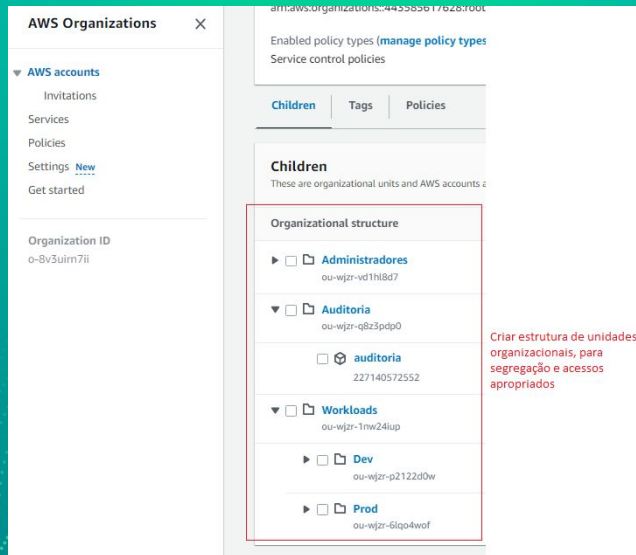
- Para evitar novos ataques, é necessário realizar uma análise minuciosa das evidências coletadas para identificação das vulnerabilidades e aplicar os ajustes necessários

Aplicar ajustes



- O AWS Organizations é um serviço global, sem custos adicionais que permite agrupar várias contas da AWS em unidades organizacionais, e aplicar políticas de segurança (Service control policies) compulsórias às contas membros, aumentando significativamente o nível de segurança

Aplicar ajustes



- É uma boa prática, utilizar uma conta exclusivamente para gerenciamento (sem alocação de serviços)
- É recomendável centralizar os logs do Cloud Trail (das contas membro) em uma conta exclusiva para esta finalidade com acessos limitados a gravação e consulta, impedindo a exclusão de registros.
- Mesmo que uma conta tenha sido comprometida, o invasor será impedido de alterar os registros de log para mascarar o ataque

Aplicar ajustes

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAllOutEast1",
      "Effect": "Deny",
      "NotAction": [
        {
          "a4b:*",
          "budgets:*",
          "ce:*",
          "chime:*",
          "cloudfront:*",
          "cur:*",
          "globalaccelerator:*",
          "health:*",
          "iam:*",
          "importexport:*",
          "mobileanalytics:*",
          "organizations:*",
          "route53:*",
          "shield:*",
          "support:*",
          "trustedadvisor:*",
          "waf:*",
          "wellarchitected:*"
        ]
      ],
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": [
            "us-east-1"
          ]
        }
      ]
    }
  ]
}
```

Liberar apenas os serviços
globais

Permitir a criação de
recurso apenas nas
regiões relacionadas

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyLeaveOrg",
      "Effect": "Deny",
      "Action": [
        "organizations:LeaveOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

Exemplos de Service Control Police:

- Restringir a criação de serviços às regiões utilizadas, bloqueando todas as demais
- Impedir as contas membros de deixar a organização

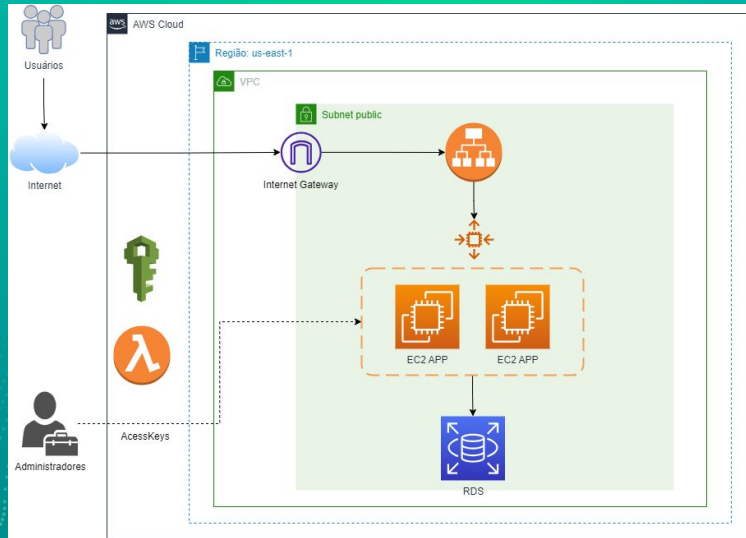
Aplicar ajustes

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RequireMicroInstanceType",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ec2:InstanceType": [
            "m5.large",
            "m5.xlarge"
          ]
        }
      }
    }
  ]
}
```

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Deny",
      "Action": [
        "ec2:*"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "ForAllValues:StringLike": {
          "aws:PrincipalArn": [
            "arn:aws:iam::*:root"
          ]
        }
      }
    }
  ]
}
```

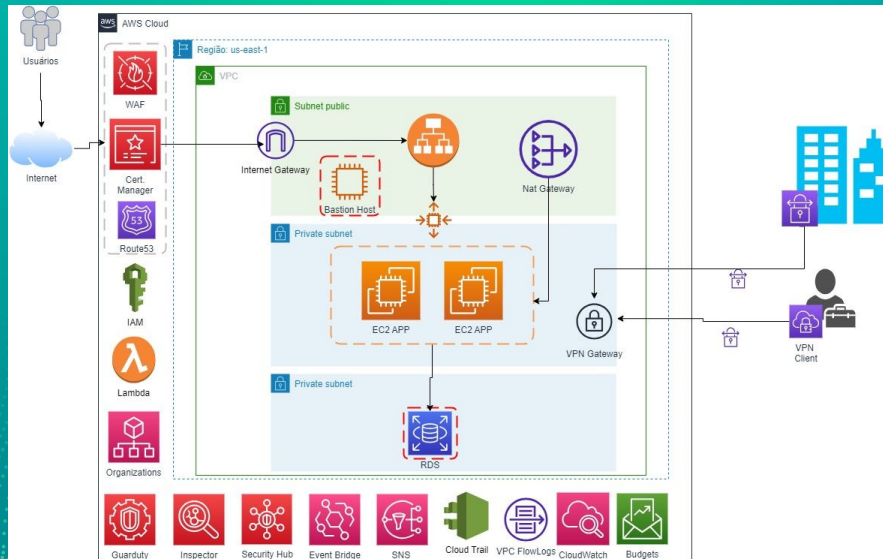
- Definir os tipos de instâncias que podem ser utilizadas
- Limitar as ações que podem ser executadas pela conta root
- Documentação e exemplos de uso:
 - https://docs.aws.amazon.com/organizations/latest/userguide/orgs_introduction.html
 - https://docs.aws.amazon.com/organizations/latest/userguide/orgs_getting-started.html

Aplicar ajustes



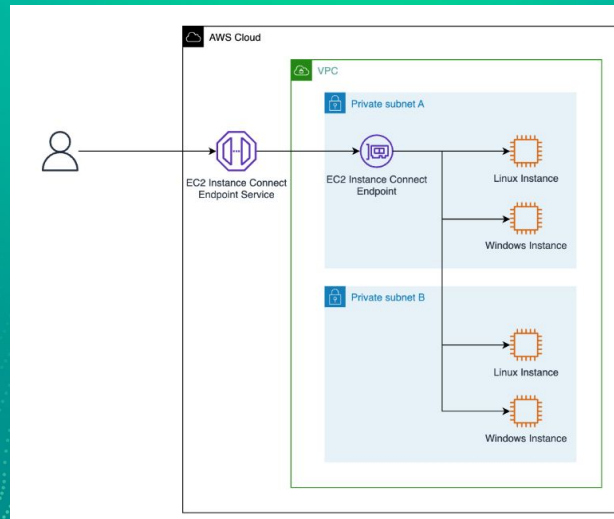
- Diagrama da estrutura original utilizada pela startup

Aplicar ajustes



- Aplicação de ajustes:
 - Alocar instâncias/aplicação e banco de dados em subnets privadas
 - Utilizar VPN ou instâncias de bastion host para administração da estrutura de forma segura
 - Ativar e configurar firewall alinhado com os serviços em uso
 - O GuardDuty é um excelente serviço baseado em machine learning que possibilita a identificação de atividades suspeitas na estrutura e pode ser integrado com outros serviços (EventBridge, WAF, SNS) para executar ações automáticas para contenção de ameaças (<https://aws.amazon.com/pt/guardduty/>)
 - A configuração de um orçamento baseado no histórico das contas em uso, pode auxiliar a identificar anormalidades na utilização dos serviços (<https://aws.amazon.com/pt/aws-cost-management/aws-budgets/>)

Aplicar ajustes



- Recentemente a AWS disponibilizou mais um serviço para acesso seguro às instâncias alocadas em subnet privadas: o EC2 Instance Connect Endpoint (<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/connect-using-eice.html>)



Roubo de dados CapitalOne

Roubo de dados CapitalOne



A Case Study of the Capital One Data Breach (Revised)

Nelson Novaes Neto, Stuart Madnick,
Anchises Moraes G. de Paula, Natasha Malara Borges

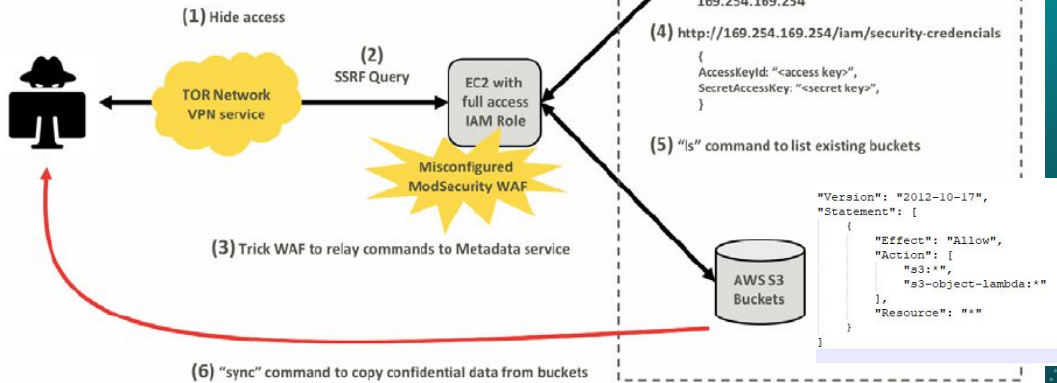
- Este estudo de caso foi baseado no artigo elaborado pela equipe de pesquisadores do banco C6 e publicado pelo MIT
<https://web.mit.edu/smadnick/www/wp/2020-16.pdf>

Roubo de dados CapitalOne

- 5º maior banco dos EUA
 - 50.000 colaboradores
 - 85% da equipe de TI formada por engenheiros
- Um dos primeiros bancos a migrar sua infraestrutura para cloud
 - Segmento altamente regulado
 - Balizamento de risco equivalente ao on-premise antes da migração para cloud

Roubo de dados CapitalOne

```
curl -s http://url/latest/meta-data/iam/security-credentials/credential \
-H "Host: 169.254.169.254"
```



- O ataque explorou a vulnerabilidade de Server-Side Request Forgery (SSRF), (2) que devido a uma falha de configuração do firewall (3), permitiu redirecionar uma url para o IP utilizado para consulta do metadata de instâncias da AWS (169.254.169.254), possibilitando à atacante capturar o AccessKeys, SecretKey e token da role configurada na instância (4)
- A credencial foi configurada via CLI no computador a atacante, que foi utilizada para realizar o acesso programático da instância, que também possuía uma Role, com acesso a todos os buckets do banco (5)
- A atacante utilizou o comando sync, para realizar o download dos dados para seu computador (6)

Roubo de dados CapitalOne

- Incidente: 22 e 23/03/2019
 - 30 GB de dados de 700 buckets
 - 106 milhões de clientes
 - 100 milhões EUA
 - 6 milhões Canadá
- Nenhum dos sistemas de segurança da organização identificou o ataque

Roubo de dados CapitalOne



- O ataque apenas chegou ao conhecimento da equipe de segurança do banco após 4 meses, quando a divisão de bug bounty recebeu o e-mail (imagem acima) de um usuário informando que identificou informações do banco em um repositório do git
- Só então a equipe de segurança interna e o FBI foi acionado para investigar o incidente

Roubo de dados CapitalOne



- **Paige Thompson**
 - Ex-colaboradora da AWS
 - Mais de 30 empresas foram afetadas:
 - Agências de governo
 - Grupos de telecomunicações
 - Universidades

Roubo de dados CapitalOne

- **Principais causas do incidente**
 - Falha de configuração do firewall
 - Bloquear tráfego de redes anônimas
 - Ativar regras de proteção contra SSRF
 - Escalação de privilégios
 - Restringir acesso apenas ao bucket necessário
 - Impedir acesso de IPs externos
 - Exfiltração de dados
 - Bloquear tráfego de saída não autorizado
 - Monitorar tráfego de saída de ambiente AWS
 - Utilização de DLP (Data Leak Prevention)

Roubo de dados CapitalOne

Stage	Step of the attack	ATT&CK
Command and Control	Use TOR to hide access	T1188 - Multi-hop Proxy (MITRE, 2018)
Initial Access	Use SSRF attack to run commands	T1190 - Exploit Public-Facing Application (MITRE, 2018)
Initial Access	Exploit WAF misconfiguration to relay the commands to the AWS metadata service	Classification unavailable ⁹
Initial Access	Obtain access credentials (AccessKeyId and SecretAccessKey)	T1078 - Valid Accounts (MITRE, 2017)
Execution	Run commands in the AWS command line interface (CLI)	T1059 - Command-Line Interface (MITRE, 2017)
Discovery	Run commands to list the AWS S3 Buckets	T1007 - System Service Discovery (MITRE, 2017)
Exfiltration	Use the sync command to copy the AWS bucket data to a local machine	T1048 - Exfiltration Over Alternative Protocol (MITRE, 2017)

- A imagem acima retirada do framework MITRE ATT&CK demonstra o mapeamento do ataque utilizado e os controles que podem ser utilizados para sua mitigação
<https://attack.mitre.org/>

Roubo de dados CapitalOne

T1090.3
Multi-hop Proxy

Mitigations

ID	Mitigation	Description
M1037	Filter Network Traffic	Traffic to known anonymity networks and C2 infrastructure can be blocked through the use of network allow and block lists. It should be noted that this kind of blocking may be circumvented by other techniques like Domain Fronting.

Detection

ID	Data Source	Data Component	Detects
DS0029	Network Traffic	Network Connection Creation	Monitor for newly constructed network connections that are sent or received by untrusted hosts.
		Network Traffic Content	Monitor and analyze traffic patterns and packet inspection associated to protocol(s) that do not follow the expected protocol standards and traffic flows (e.g extraneous packets that do not belong to established flows, gratuitous or anomalous traffic patterns, anomalous syntax, or structure). Consider correlation with process monitoring and command line to detect anomalous processes execution and command line arguments associated to traffic patterns (e.g. monitor anomalies in use of files that do not normally initiate connections for respective protocol(s)).

Roubo de dados CapitalOne

Stage	Step of the attack	Technical Controls	CSF NIST Failed Controls
Command And Control	Use TOR Network to hide the origin of the attack	Block at Firewall and hosts access from IP addresses from TOR network exit nodes and from malicious proxy server. Alert on IDS/IPS successful access from malicious IP addresses.	ID.AM-4: External information systems are catalogued PR.DS-5: Protections against data leaks are implemented DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed DE.CM-1: The network is monitored to detect potential cybersecurity events DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed DE.DP-2: Detection activities comply with all applicable requirements
Initial Access	Use SSRF attack to run commands on vulnerable server	Such attack could be mitigated by a well configured WAF and preventive controls, such as periodic vulnerability scanners.	PR.IP-12: A vulnerability management plan is developed and implemented PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities DE.AE-3: Event data are collected and correlated from multiple sources and sensors DE.CM-1: The network is monitored to detect potential cybersecurity events DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events DE.CM-7: Monitoring for unauthorized personnel, connections,

- Controles do framework NIST para mitigação do ataque utilizado <https://www.nist.gov/>

PR.DS-5: Protections against data leaks are **NIST Special Publication 800-53 Revision 5**

AC-4: Information Flow Enforcement

Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on [Assignment: organization-defined information flow control policies].

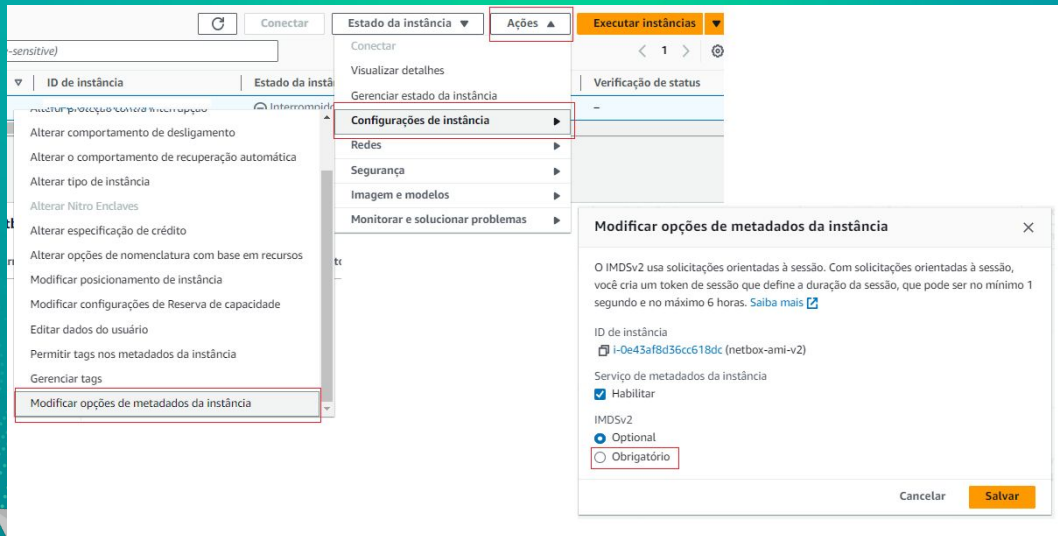
AC-5: Separation of Duties

Identify and document [Assignment: organization-defined duties of individuals requiring separation]; and Define system access authorizations to support separation of duties.

Roubo de dados CapitalOne

Stage	Step of the attack	Technical Controls	CSF NIST Failed Controls
Exfiltration	Use the sync command to copy data from AWS buckets to local computer	Outbound traffic monitoring	<p>ID.AM-3: Organizational communication and data flows are mapped</p> <p>PR.AC-3: Remote access is managed</p> <p>PR.DS-1: Data-at-rest is protected</p> <p>PR.DS-5: Protections against data leaks are implemented</p> <p>PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy</p> <p>PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities</p> <p>DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed</p> <p>DE.AE-3: Event data are collected and correlated from multiple sources and sensors</p> <p>DE.CM-1: The network is monitored to detect potential cybersecurity events</p> <p>DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events</p> <p>DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed</p> <p>DE.DP-2: Detection activities comply with all applicable requirements</p>

Habilitar Metadata v2



- Após o incidente com o Capital One, a AWS criou a versão 2 do Metadata, que impede o acesso aos dados da AccessKey que foram essenciais para a deflagração do ataque
- No entanto, por questões de compatibilidade, este recurso vem desabilitado por padrão na maioria das instâncias, obrigando ao usuário executar intervenção manual para sua ativação

Conclusão

Conclusão

- **Medidas de prevenção:**
 - Entender o cenário antes de iniciar a migração/deploy
 - Utilizar frameworks para validação da estrutura de segurança:
 - MITRE ATT&CK
 - NIST
 - Realizar pentest/auditoria regularmente
 - Elaborar plano de resposta a incidentes
 - Configurar alertas de atividades suspeitas
 - Manter inventário atualizado e documentado
 - Segurança camadas (Firewall, SG, VPCs, Auditoria)
 - Bloquear recursos não utilizados
 - Não utilizar a conta root
 - Aplicar princípio do mínimo privilégio (contas, roles, serviços)
 - Não utilizar configurações default (Metadata v2)



Obrigado

O preço da paz é a eterna vigilância

John Philpot Curran



Pedro Borges

pedroeborges@gmail.com

in /pedroborgescio

