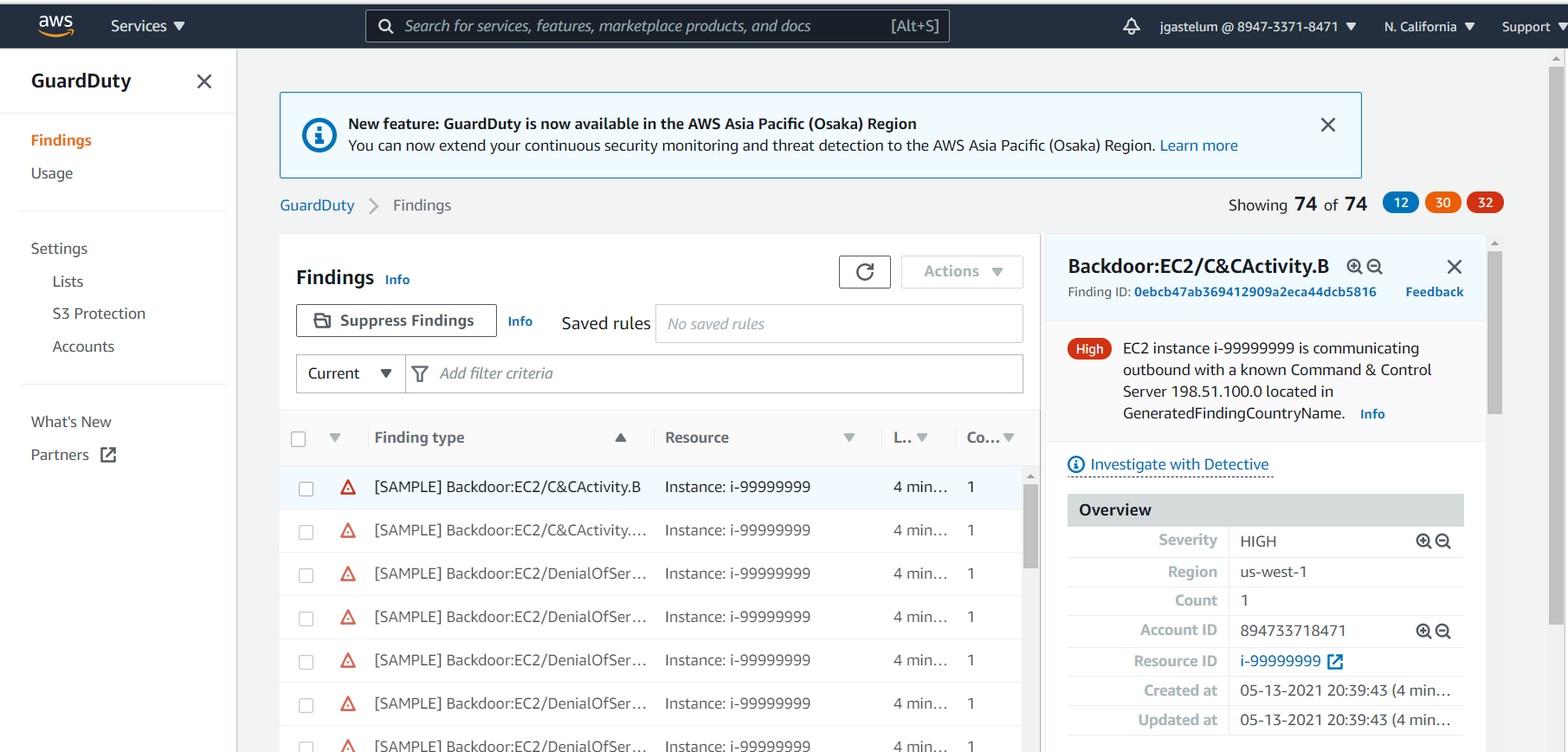
1)



1)What is the Finding Type?  
EC2 instance i-99999999 is communicating outbound with a known Command & Control Server 198.51.100.0 located in GeneratedFindingCountryName.

2)What does it mean for this finding to have occurred?  
This finding informs you that the listed instance within your AWS environment is querying an IP associated with a known command and control (C&C) server. The listed instance might be compromised. Command and control servers are computers that issue commands to members of a botnet. A botnet is a collection of internet-connected devices which might include PCs, servers, mobile devices, and Internet of Things devices, that are infected and controlled by a common type of malware. Botnets are often used to distribute malware and gather misappropriated information, such as credit card numbers. Depending on the purpose and structure of the botnet, the C&C server might also issue commands to begin a distributed denial-of-service (DDoS) attack.

3)What resource was affected, the resource ARN?  
arn:aws:outposts:us-west-2:123456789000:outpost/op-0fbc006e9abbc73c3

4)What is the finding risk level?  
High

5)If it is an instance, what is the Public IP?   
198.51.100.0

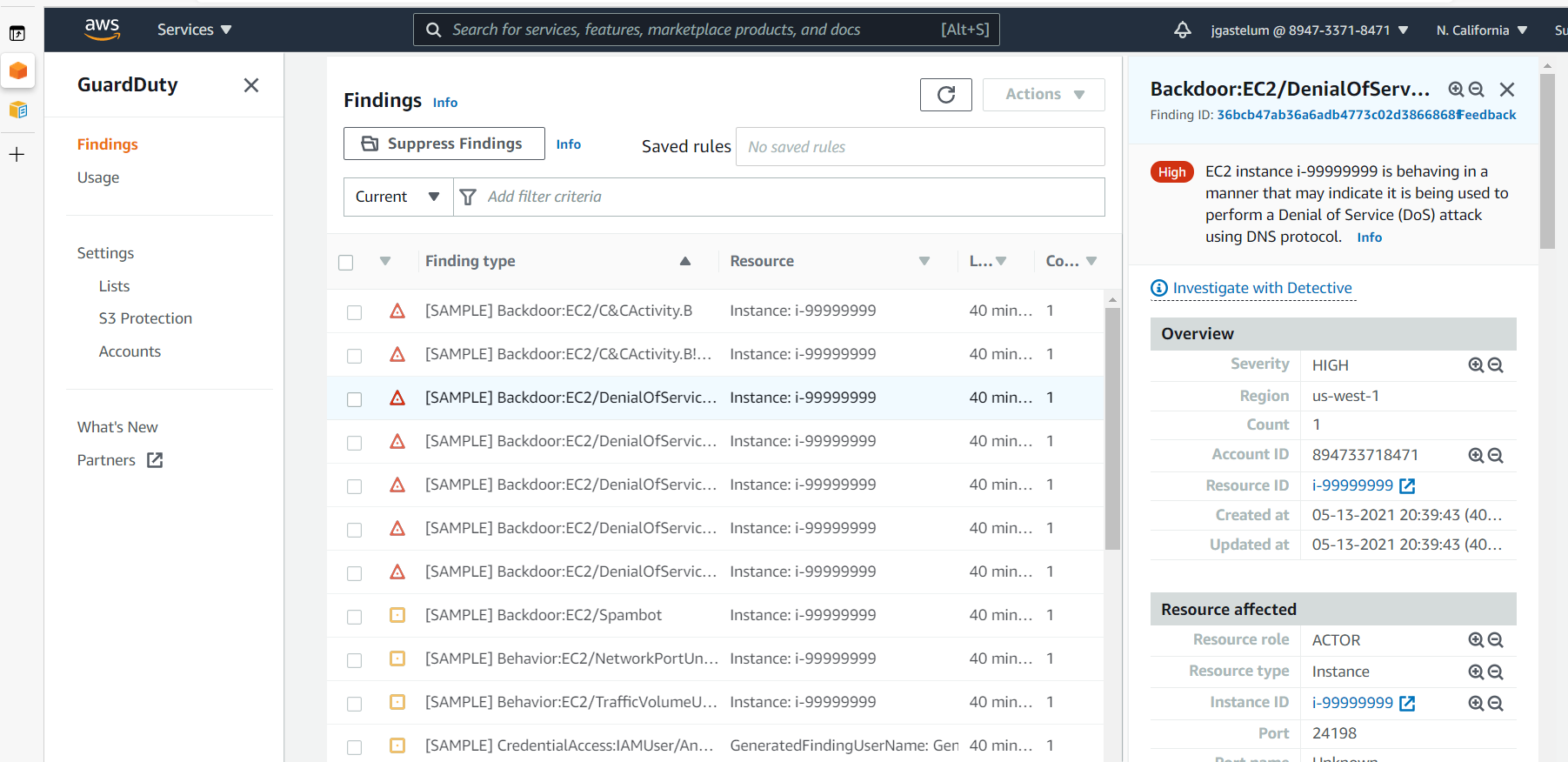
6)What steps should be done to provident this Finding to occur again?

In reference to this link: https://docs.aws.amazon.com/guardduty/latest/ug/guardduty\_remediate.html?icmpid=docs\_gd\_help\_panel#compromised-ec2

Remediating a compromised EC2 instance

Follow these recommended steps to remediate a compromised EC2 instance in your AWS environment:

* Investigate the potentially compromised instance for malware and remove any discovered malware. You can also refer to the [AWS Marketplace](https://aws.amazon.com/marketplace) for partner products that might help to identify and remove malware.
* If you are unable to identify and stop unauthorized activity on your EC2 instance, we recommend that you terminate the compromised EC2 instance and replace it with a new instance as needed. The following are additional resources for securing your EC2 instances:
  + "Security and Network" section in [Best practices for amazon EC2](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-best-practices.html).
  + [Amazon EC2 security groups for Linux instances](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html) and [Amazon EC2 security groups for Windows instances](https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/using-network-security.html).
  + [Tips for securing your EC2 instances (Linux)](http://aws.amazon.com/articles/tips-for-securing-your-ec2-instance/).
  + [AWS security best practices](https://aws.amazon.com/architecture/security-identity-compliance/)
* Browse for further assistance on the AWS developer forums: <https://forums.aws.amazon.com/index.jspa>
* If you are a Premium Support package subscriber, you can submit a [technical support](https://console.aws.amazon.com/support/home#/case/create?issueType=technical) request.

2) 

1)What is the Finding Type?

EC2 instance i-99999999 is behaving in a manner that may indicate it is being used to perform a Denial of Service (DoS) attack using DNS protocol.

2)What does it mean for this finding to have occurred?

This finding informs you that the listed EC2 instance within your AWS environment is generating a large volume of outbound DNS traffic. This may indicate that the listed instance is compromised and being used to perform denial-of-service (DoS) attacks using DNS protocol.

* **Note:** This finding detects DoS attacks only against publicly routable IP addresses, which are primary targets of DoS attacks.

3)What resource was affected, the resource ARN?

arn:aws:outposts:us-west-2:123456789000:outpost/op-0fbc006e9abbc73c3

4)What is the finding risk level?

High

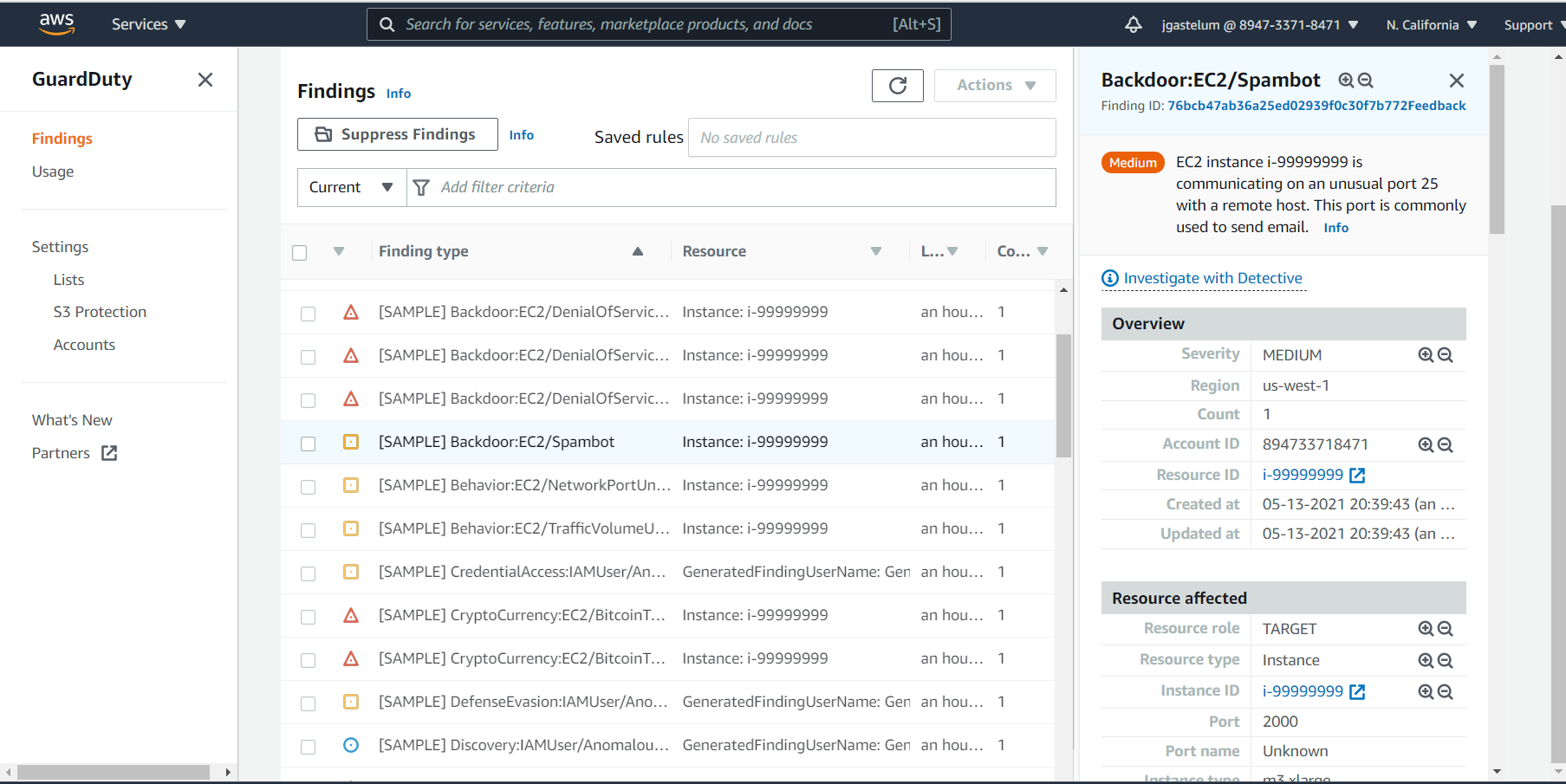
5)If it is an instance, what is the Public IP?   
198.51.100.0

## 6)What steps should be done to provident this Finding to occur again? In reference to this link: https://docs.aws.amazon.com/guardduty/latest/ug/guardduty\_remediate.html?icmpid=docs\_gd\_help\_panel#compromised-ec2 Remediating a compromised EC2 instance

Follow these recommended steps to remediate a compromised EC2 instance in your AWS environment:

* Investigate the potentially compromised instance for malware and remove any discovered malware. You can also refer to the [AWS Marketplace](https://aws.amazon.com/marketplace) for partner products that might help to identify and remove malware.
* If you are unable to identify and stop unauthorized activity on your EC2 instance, we recommend that you terminate the compromised EC2 instance and replace it with a new instance as needed. The following are additional resources for securing your EC2 instances:
  + "Security and Network" section in [Best practices for amazon EC2](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-best-practices.html).
  + [Amazon EC2 security groups for Linux instances](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html) and [Amazon EC2 security groups for Windows instances](https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/using-network-security.html).
  + [Tips for securing your EC2 instances (Linux)](http://aws.amazon.com/articles/tips-for-securing-your-ec2-instance/).
  + [AWS security best practices](https://aws.amazon.com/architecture/security-identity-compliance/)
* Browse for further assistance on the AWS developer forums: <https://forums.aws.amazon.com/index.jspa>
* If you are a Premium Support package subscriber, you can submit a [technical support](https://console.aws.amazon.com/support/home#/case/create?issueType=technical) request.

3)



1)What is the Finding Type?

EC2 instance i-99999999 is communicating on an unusual port 25 with a remote host. This port is commonly used to send email.

2)What does it mean for this finding to have occurred?  
This finding informs you that the listed EC2 instance in your AWS environment is communicating with a remote host on port 25. This behavior is unusual because this EC2 instance has no prior history of communications on port 25. Port 25 is traditionally used by mail servers for SMTP communications. This finding indicates your EC2 instance might be compromised for use in sending out spam.

3)What resource was affected, the resource ARN?  
arn:aws:outposts:us-west-2:123456789000:outpost/op-0fbc006e9abbc73c3

4)What is the finding risk level?

Medium

5)If it is an instance, what is the Public IP?   
198.51.100.0

6)What steps should be done to provident this Finding to occur again?  
In reference to the link: https://docs.aws.amazon.com/guardduty/latest/ug/guardduty\_remediate.html?icmpid=docs\_gd\_help\_panel#compromised-ec2

Remediating a compromised EC2 instance

Follow these recommended steps to remediate a compromised EC2 instance in your AWS environment:

* Investigate the potentially compromised instance for malware and remove any discovered malware. You can also refer to the [AWS Marketplace](https://aws.amazon.com/marketplace) for partner products that might help to identify and remove malware.
* If you are unable to identify and stop unauthorized activity on your EC2 instance, we recommend that you terminate the compromised EC2 instance and replace it with a new instance as needed. The following are additional resources for securing your EC2 instances:
  + "Security and Network" section in [Best practices for amazon EC2](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-best-practices.html).
  + [Amazon EC2 security groups for Linux instances](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html) and [Amazon EC2 security groups for Windows instances](https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/using-network-security.html).
  + [Tips for securing your EC2 instances (Linux)](http://aws.amazon.com/articles/tips-for-securing-your-ec2-instance/).
  + [AWS security best practices](https://aws.amazon.com/architecture/security-identity-compliance/)
* Browse for further assistance on the AWS developer forums: <https://forums.aws.amazon.com/index.jspa>
* If you are a Premium Support package subscriber, you can submit a [technical support](https://console.aws.amazon.com/support/home#/case/create?issueType=technical) request.

6)

