Examples of Email Sent to AWS Root Account Addresses and AWS Security Contacts

Example 1

From: Amazon EC2 Abuse <ec2-abuse@amazon.com>
Reply-To: Amazon EC2 Abuse <ec2-abuse@amazon.com>
Date: Wednesday, February 28, 2018 at 12:18 PM
To: ROOT_ACCOUNT_SECURITY_CONTACT
Cc: ROOT_ACCOUNT_EMAIL_ADDRESS
Subject: Your Amazon EC2 Abuse Report [12345678901-1] [AWS ID 123456789012]

Hello,

We've received a report(s) that your AWS resource(s)

AWS ID: 123456789012 Region: us-east-1 EC2 Instance Id: i-6666666

has been implicated in activity which resembles scanning hosts on the internet for security vulnerabilities. If you are aware of this activity and you are conducting security testing (penetration tests, vulnerability scanning), or any other type of simulated event, please be sure to request an exception to prevent further abuse notices. You can submit your request at the following link:
https://aws.amazon.com/security/penetration-testing/

If you're unaware of this activity, it's possible that your environment has been compromised by an external attacker, or a vulnerability is allowing your machine to be used in a way that it was not intended.

For guidance on securing your instance, we recommend reviewing the following resources:

* Amazon EC2 Security Groups User Guide:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html (Linux)
https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/using-network-security.html (Windows)

* Tips for Securing EC2 Instances:
https://aws.amazon.com/articles/1233 (Linux)
https://aws.amazon.com/articles/1767 (Windows)

* AWS Security Best Practices:
https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf

If you require further assistance with this matter, you can take advantage of our developer forums:
https://forums.aws.amazon.com/index.jspa

Or, if you are subscribed to a Premium Support package, you may reach out for one-on-one assistance here:
https://console.aws.amazon.com/support/home#/case/create?issueType=technical

This report is informational only, no further follow up is required on your part. Please remember that you are responsible for ensuring that your instances and all applications are properly secured. If you require any further information to assist you in identifying or rectifying this issue, please let us know in a direct reply to this message.

Regards,
AWS Abuse

Abuse Case Number: 12345678901-1

---Beginning of forwarded report(s)---

* Log Extract:
<<<
AWS Account: 123456789012
Report begin time: 28-02-2018 17:03:12 UTC
Report end time: 28-02-2018 17:04:12 UTC

Protocol: TCP
Remote IP: 11.22.33.44
Remote port(s): multiple ports (1000 ports in total)

Total bytes sent: 119357
Total packets sent: 2023
Total bytes received: 360
Total packets received: 6

>>>

* Comments:
<<<

>>>

How can I contact a member of the Amazon EC2 abuse team or abuse reporter?
Reply this email with the original subject line.

Amazon Web Services