# CHECK POINT CLOUD CHECKUP REPORT

This report presents the findings of Check Point's security assessments conducted in your cloud environment.
The report details your organization's exposure to security threats in the cloud.

vpc-8b8bf8e2 | 15 Dec.19 11:14 - 22 Dec.19 11:14 (UTC) | 12 Monitored machines
of 32 instances discovered

## 3K Malicious Communications

124 C&C Servers

152 Infectious Connections

148 Compromised Servers

139 Volatile Servers

143 Crypto-Miners

2K Scanners

154 Phishing Websites

131 Adware Servers

## 6 Failed Practices

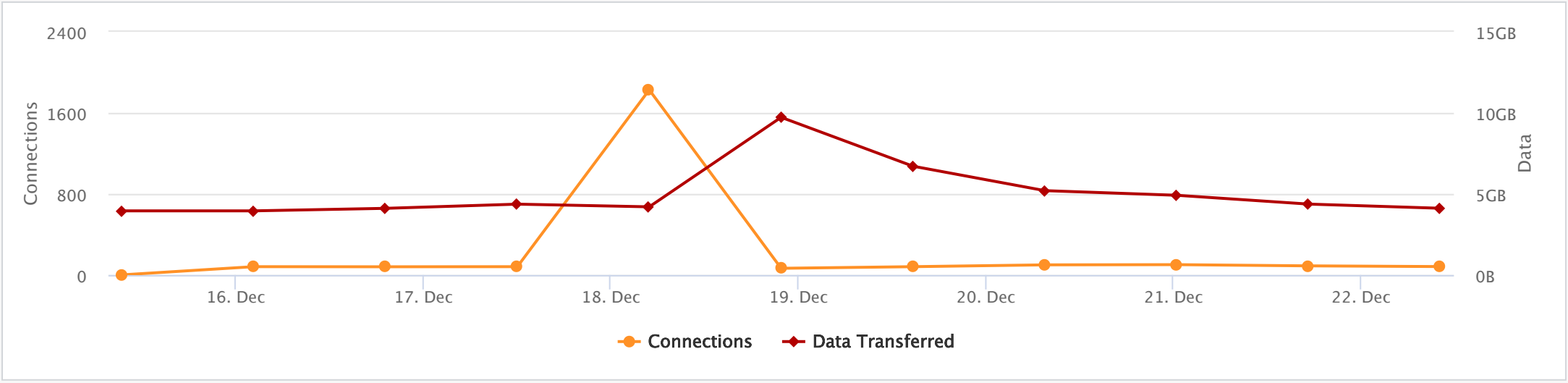
1 Compute (EC2)

2 Databases (RDS, DynamoDB)

2 Security & Identity (IAM)

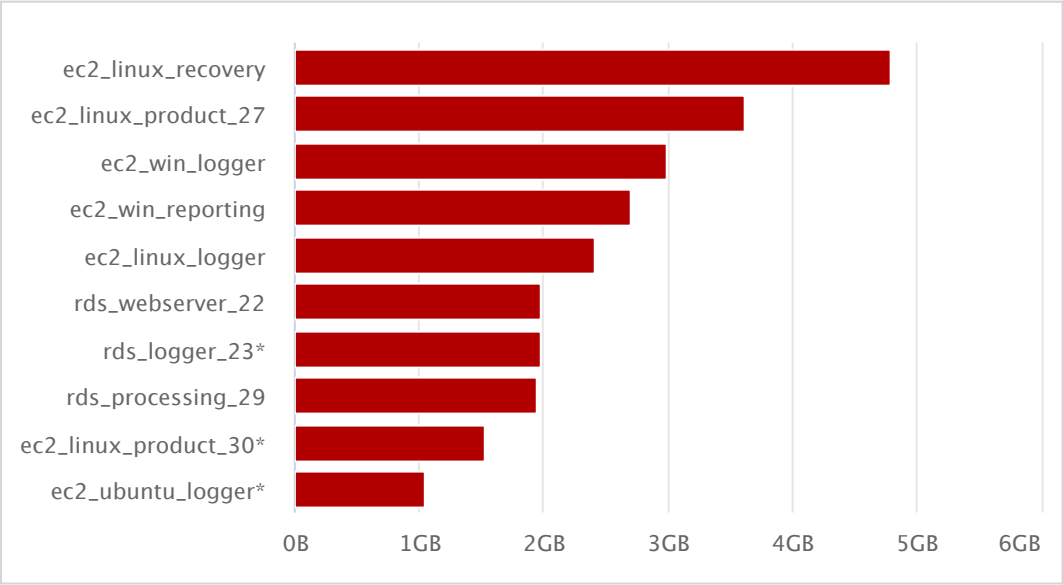
1 Storage (S3 Bucket)

## TOTAL MALICIOUS TRAFFIC



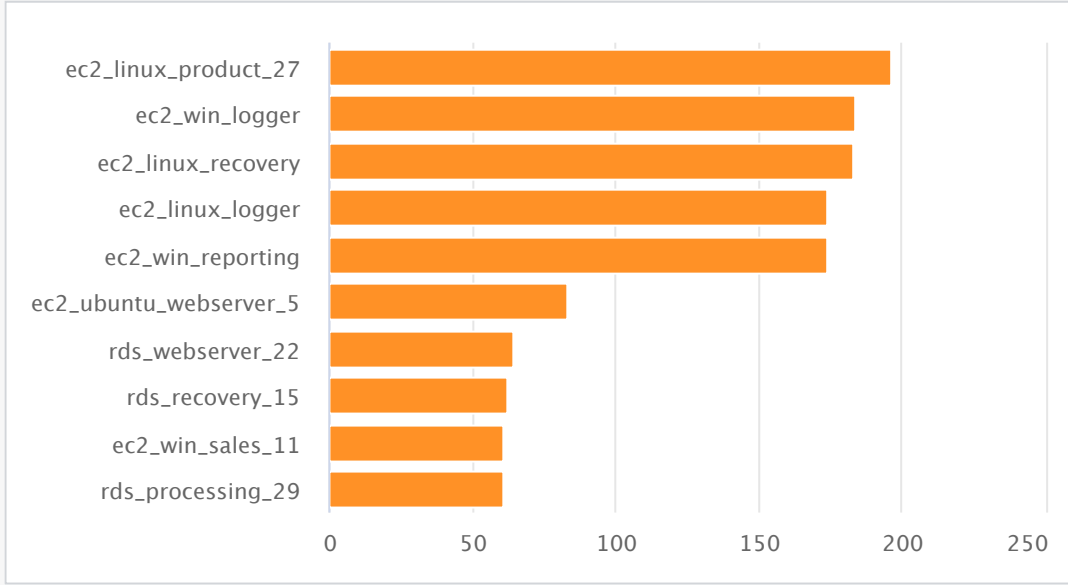

## MALICIOUS DATA TRANSFER PER MACHINE

Total of 51.74 GB




## MALICIOUS CONNECTIONS PER MACHINE

Total of 3k malicious connections




* Unmonitored Machines

## REMOTE ACCESS (SSH / RDP)

### North - South Traffic

Unique communications with different hosts over RDP and SSH

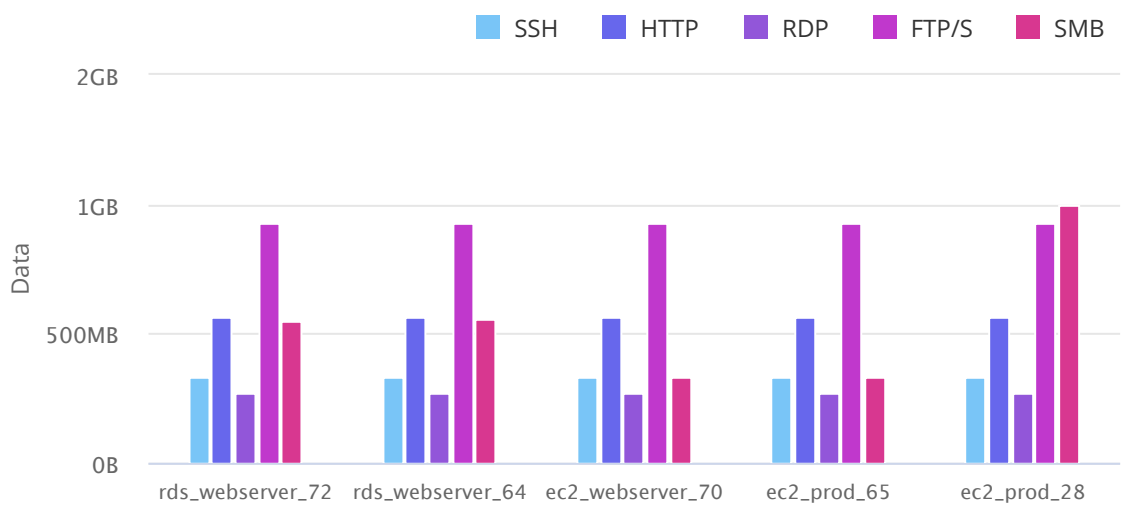
| MACHINE NAME | LOGIN ATTEMPTS | ACCESSED BY |
|---|---|---|
| ec2_linux_recovery | 3,189 | SSH |
| ec2_linux_logger | 6 | SSH |
| ec2_win_reporting | 5 | RDP, SSH |
| ec2_ubuntu_webserver_5 | 5 | RDP, SSH |
| ec2_win_sales_11 | 5 | RDP, SSH |

### East - West Traffic

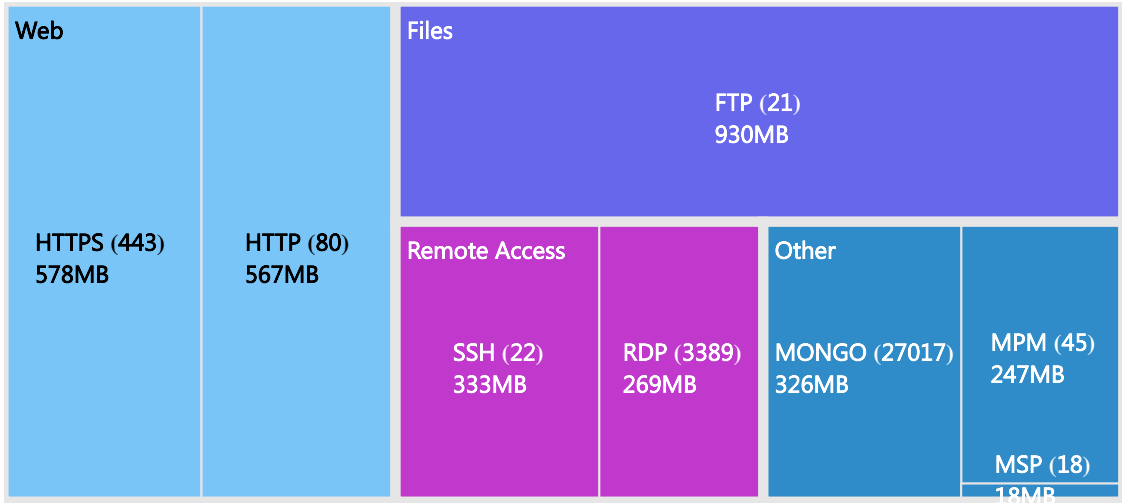
Unique communications within the VPC over RDP and SSH

| MACHINE NAME | LOGIN ATTEMPTS | ACCESSED BY |
|---|---|---|
| rds_logger_10* | 2,466 | SSH |
| ec2_prod_41* | 10 | RDP |
| rds_client_43* | 9 | SSH |
| ec2_client_82* | 4 | RDP, SSH |
| rds_webserver_72* | 3 | SSH |

## TOP 5 HIGH RISK SERVICES USED PER MACHINE




## TOTAL OF ALL SERVICES USED



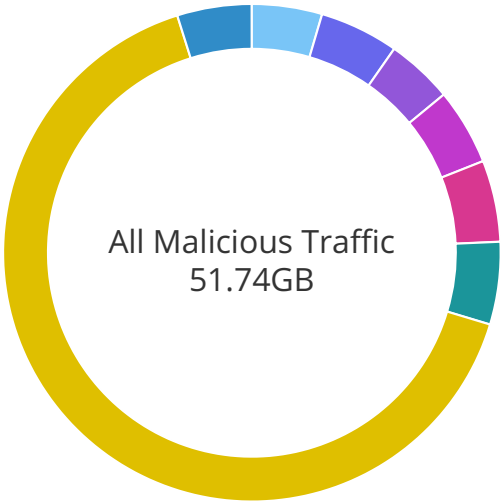
## TRAFFIC

All Traffic

8.78TB

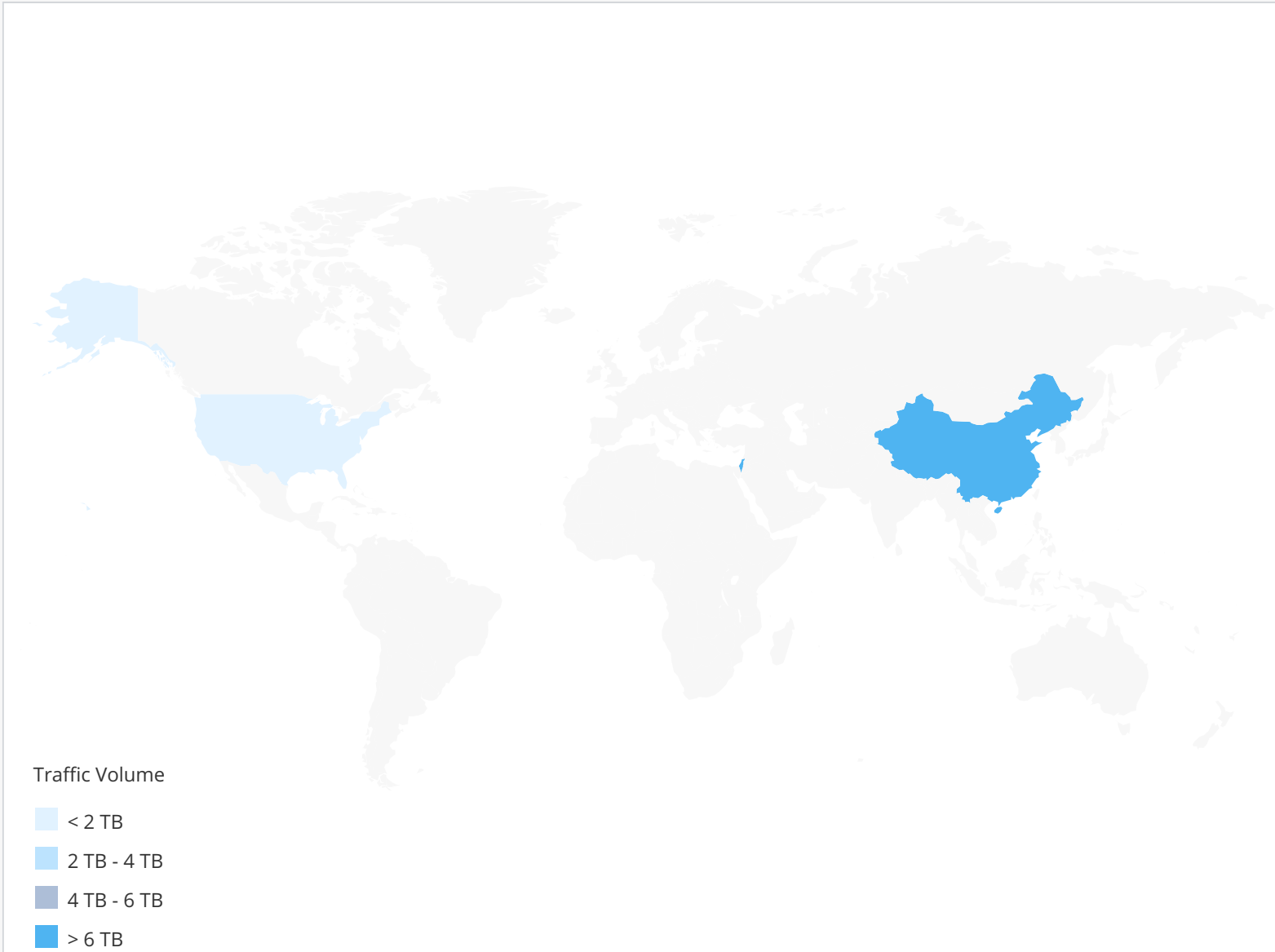
Inbound
2.63TB

Outbound
6.14TB

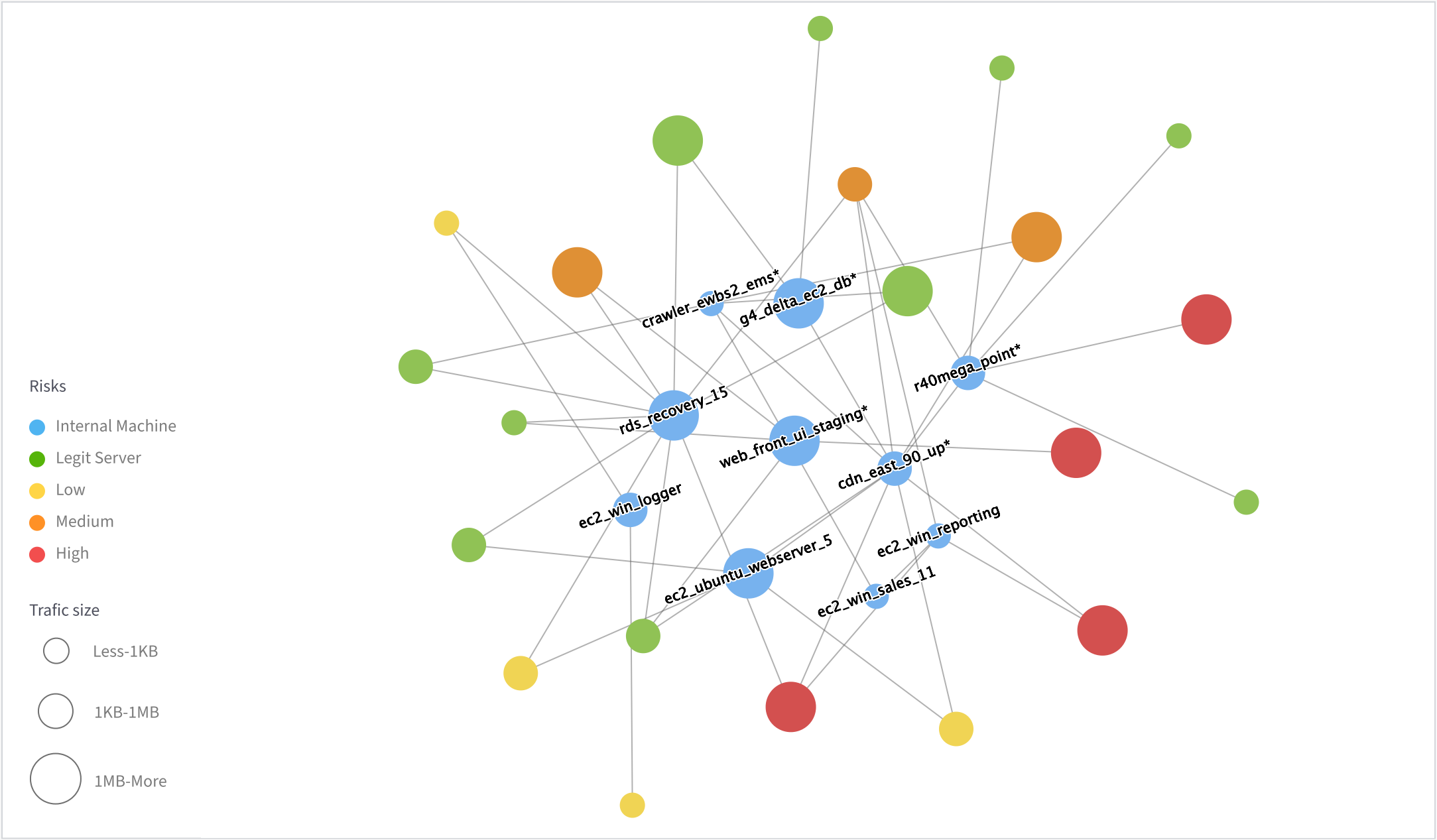



| | | |
|---|---|---|
| Adware Servers | 2.4 GB | 5% |
| Compromised Servers | 2.7 GB | 5% |
| C&C Servers | 2.2 GB | 4% |
| Crypto-Miners | 2.6 GB | 5% |
| Infectious Servers | 2.7 GB | 5% |
| Phishing Websites | 2.8 GB | 5% |
| Scanners | 33.9 GB | 66% |
| Volatile Servers | 2.5 GB | 5% |

## GEOLOCATION DISTRIBUTION OF TRAFFIC VOLUME



## NETWORK GRAPH



# 6 FAILED PRACTICES

## 1 Compute (EC2)

- Ensure AMI is not exposed to the public internet Read More...
  - Exception found at "ami-04c69...334c6fd2","ami-07a6b...3107f643","ami-0af6f...da86158b" and 1 more

## 2 Databases (RDS, DynamoDB)

- Ensure AWS DynamoDB is encrypted using AWS managed CMKs Read More...
- Ensure RDS storage is encrypted Read More...

## 2 Security & Identity (IAM)

- Ensure IAM password policy expires passwords within 90 days or less Read More...
  - Exception found at "Admin","arikl","dekely" and 7 more
- Ensure Hardware MFA is enabled for the 'root' account Read More...

## 1 Storage (S3 Bucket)

- Ensure s3 bucket access logging is enabled on the CloudTrail s3 bucket Read More...
  - Exception found at "validation-se-serverlessdeploymentbuck-vz9c81aw115o"