Amazon Web Services: Exploring the Cost of Exfil

aon.com/cyber-solutions/aon_cyber_labs/amazon-web-services-exploring-the-cost-of-exfil/

Introduction

Stroz Friedberg is often called upon by organizations to investigate matters involving unintended or unauthorized access to Amazon Web Services ("AWS"). When threat actors impact AWS or more particularly Amazon Simple Storage Service ("S3"), they always leave a trace – but the difficult part is trying to identify the who, what, where, when and why. Also, just so it is said, threat actors are not the only ones causing or exploiting issues within AWS. Stroz Friedberg has also linked what appears to be malicious activity to internal misconfigurations or mistakes by internal employees.

This article will demonstrate how Stroz Friedberg uses a free and easily accessible AWS tool known as Cost Explorer to triage AWS during investigations. Cost Explorer's primary purpose is to provide a visual representation of AWS cost and usage over time. As is usually the case in forensics and investigations, data intended for one use can provide valuable information to help fill in gaps in a storyline/timeline. In this case, Cost Explorer, while intended to provide a view of costs associated with using AWS resources, can also be used to spot unintended/unauthorized activity within an AWS environment or to triage a particular timeframe of interest. In the event you see anomalous activity, please contact Stroz Friedberg. It is imperative that you have internal or external experts working with your team in the event unintended or unauthorized activity presents itself.

Background

AWS S3 is a scalable, easy-to-use storage solution that many organizations leverage for a range of use cases, such as hosting a website, storing backups, archiving data, and data analytics. When organizations utilize the cloud to host their infrastructure or services, they must invest in adequate risk controls and cyber resilience strategies. That said, when misconfigurations or vulnerabilities are present in AWS S3, threat actors may find and exploit them. Contact Stroz Friedberg to learn more on how we can help you design, and secure AWS cloud services.

How to search for possible unintended & unauthorized AWS activity

Stroz Friedberg often leverages AWS Cost Explorer to triage AWS incidents in the preliminary stages of our AWS investigations.

So, what is AWS Cost Explorer?

AWS Cost Explorer is an embedded AWS tool that enables one to visualize cost and resource usage within your AWS account. In other words, if one were curious why their AWS bill increased since the last billing cycle, AWS Cost Explorer can help. Data stored within Cost Explorer is retained for 12 months by default. Below is a step-by-step process to leverage this historical data to identify possible exfiltration events within AWS S3.

Step 1 – Find Cost Explorer

To access the Cost Explorer visualizer tool, search for and select “Cost Explorer” in the search bar of the AWS web console or navigate to the direct link here. This will take you to the AWS Cost Management homepage. On the left side bar, select “Cost Explorer.” You will be presented with a dashboard like Figure 1 below:

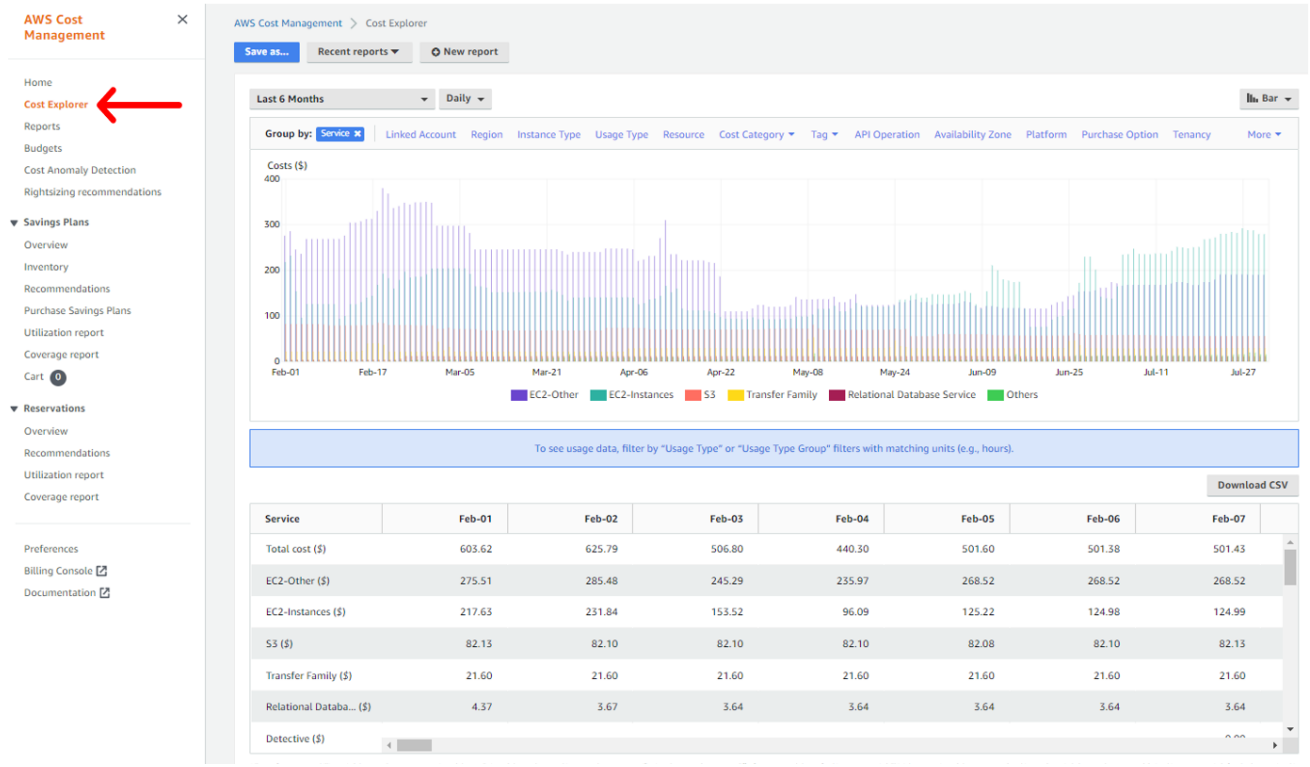


Figure 1. Cost Explorer landing page

Step 2 – Use Cost Explorer

AWS Cost Explorer is designed with the capability for the user to filter on multiple attributes which presents them with an interactive visualization of data which is typically camouflaged and/or not easily accessible. One powerful feature of Cost Explorer is one can dive in on custom time periods with various levels of specificity and granularity.

To perform an AWS S3 triage analysis with AWS Cost Explorer:

1. Specify the appropriate time period and set the interval to “Daily”.

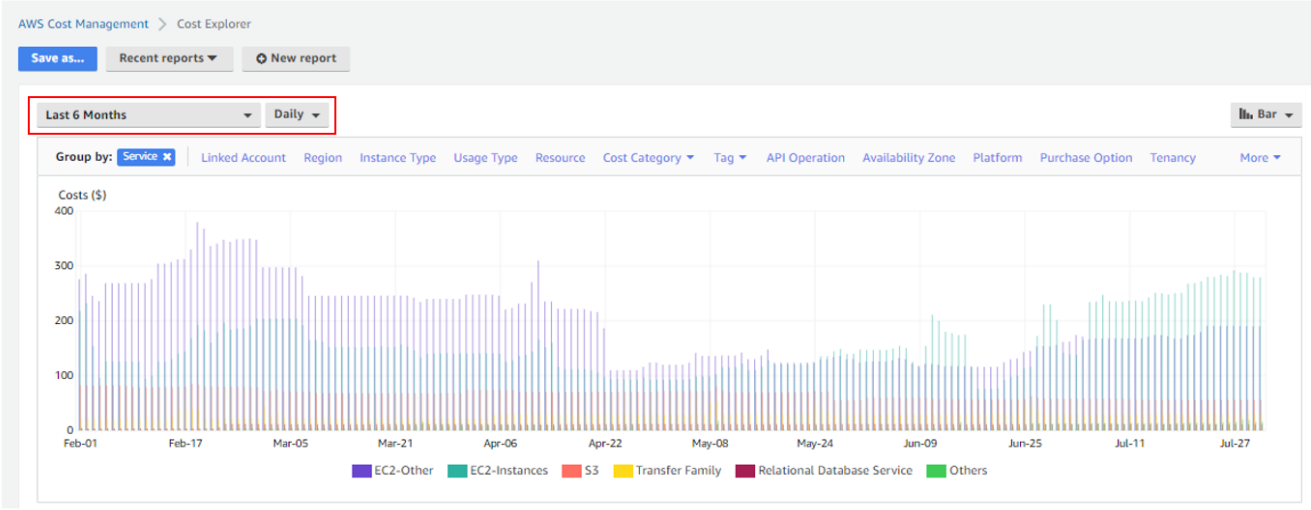


Figure 2. Timeframe and Interval filters in Cost Explorer

2. Set a filter for “S3” in the “Service” filter category.

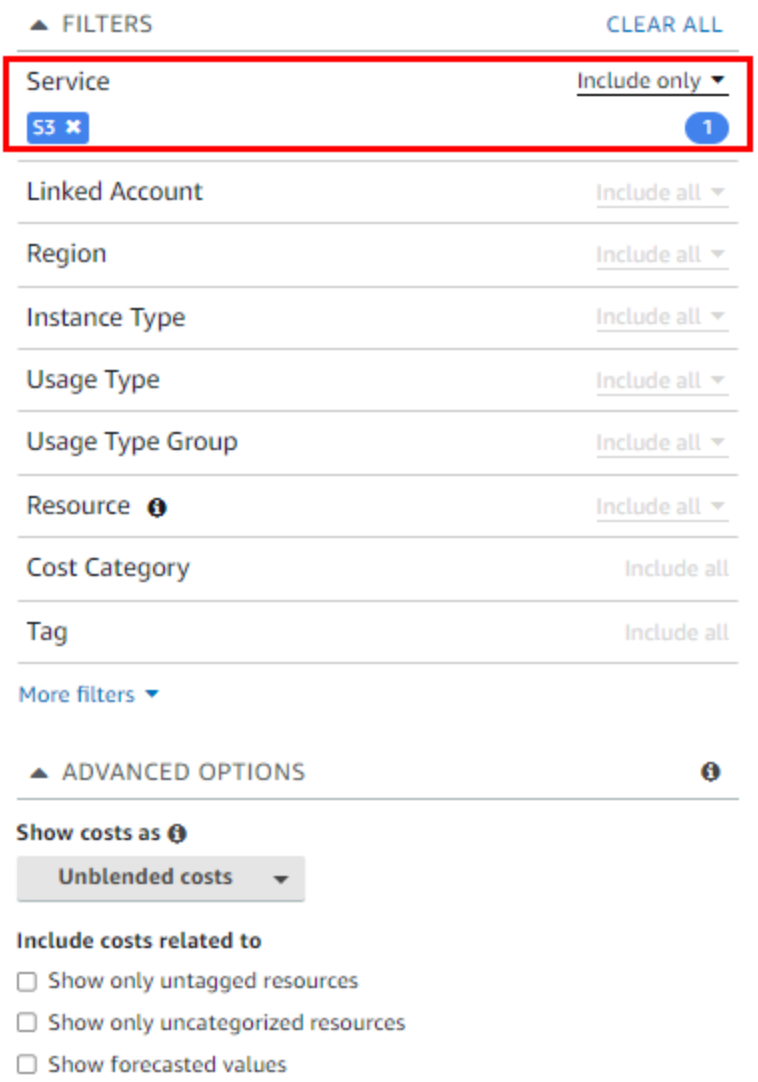


Figure 3. Cost Explorer filtered on service “S3”

3. Set the “Usage Type Group” filter to “S3: Data Transfer – Internet (Out)”.

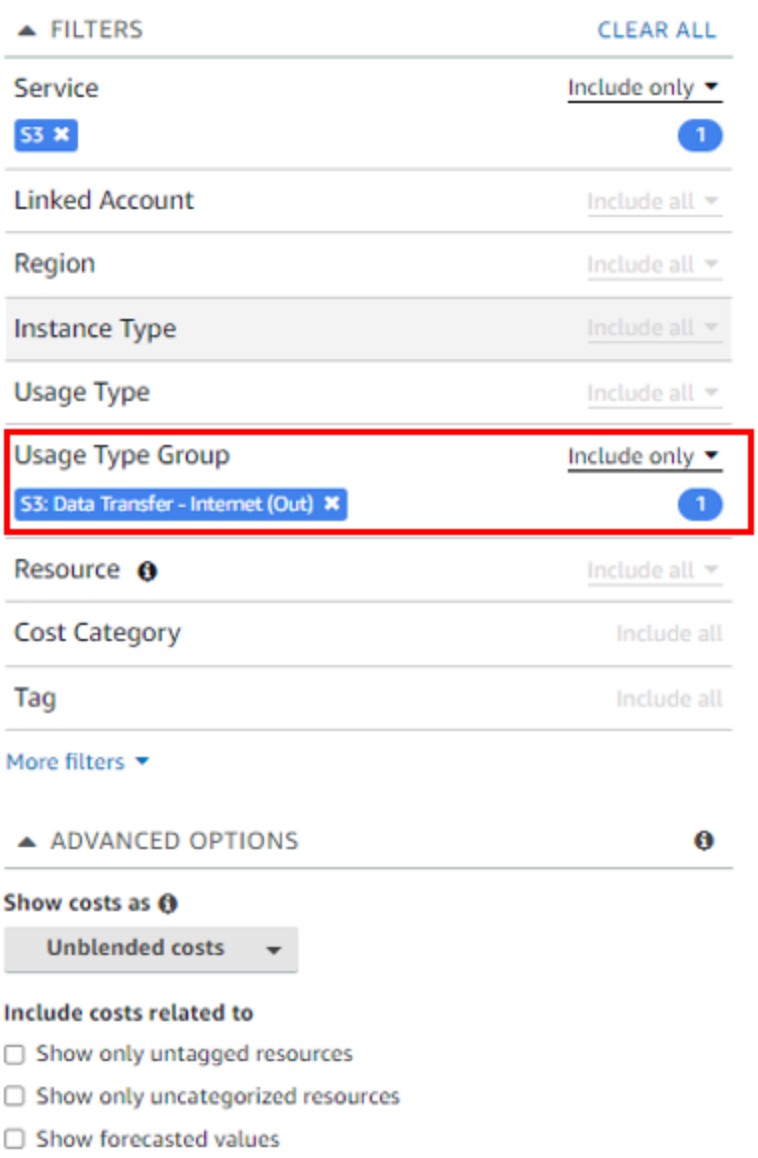


Figure 4 Cost Explorer filtered on Usage Type Group "S3: Data Transfer – Internet (Out)"

The goal of this analysis is to find an abnormality in outgoing AWS S3 data transfer activity based on historical usage within the AWS account, then determine if the activity is the result of an expected business function/behavior. In that effort, the graph below (Figure 5) shows two areas of interest:

1. The top bar graph labeled "Costs ($)" provides an overview of the cost of the AWS S3 service per day.
2. The second bar graph labeled "Usage (GB)" provides an overview of the amount of data in gigabytes ("GB") that were transferred per day.

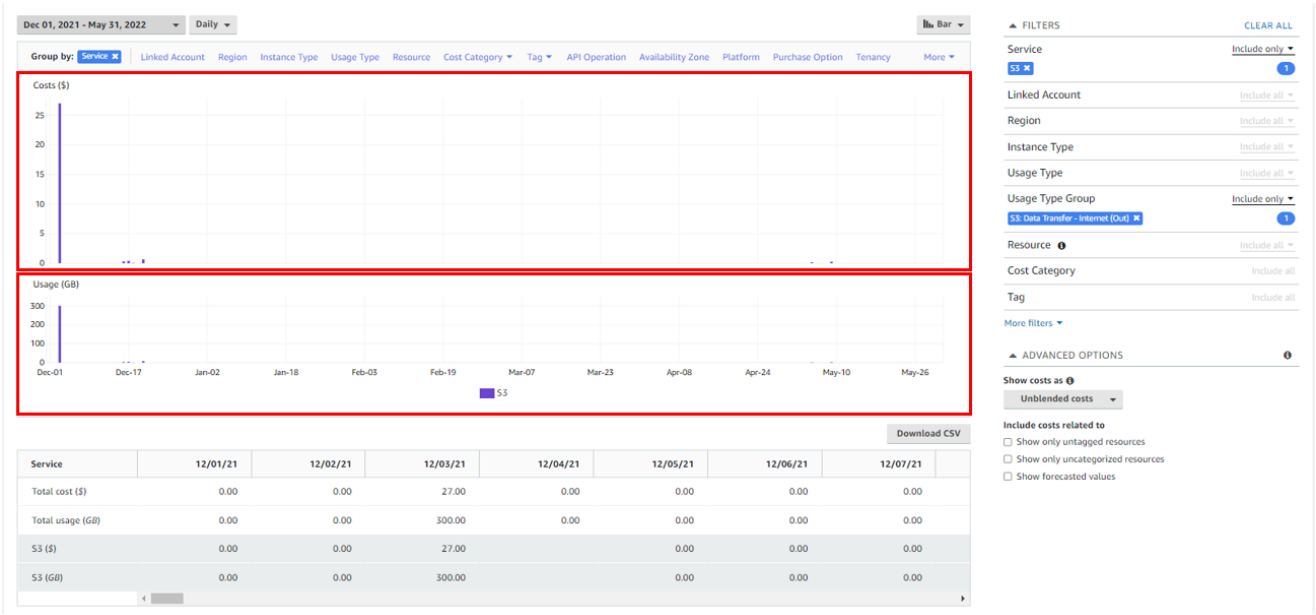


Figure 5. Example of a spike in data transferred outbound to the internet in AWS S3

Looking at the Usage graph, there is a clear spike in data usage on December 3, 2021. On this day there was a total of 300.00 GB transferred out to the internet. Compare this to the historical usage over the last six months, and it is clear a transfer of this size is abnormal behavior.

Additionally, to discover more about what happened on December 3, 2021, Cost Explorer can be further filtered on specific API ("Application Programming Interfaces") operations such as "GetObject", even when Object Access logging is not enabled. To do this apply the same filters as above, but instead of grouping by "Service" group by "API Operation" as shown by the top arrow in Figure 6.

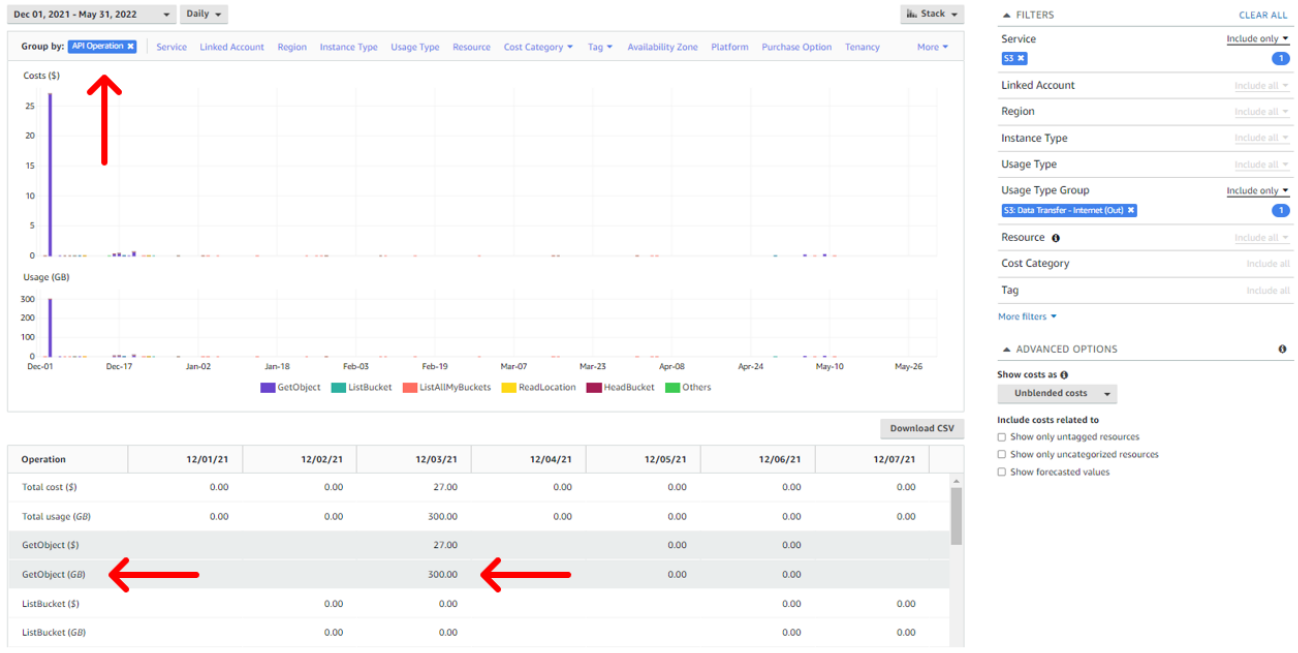
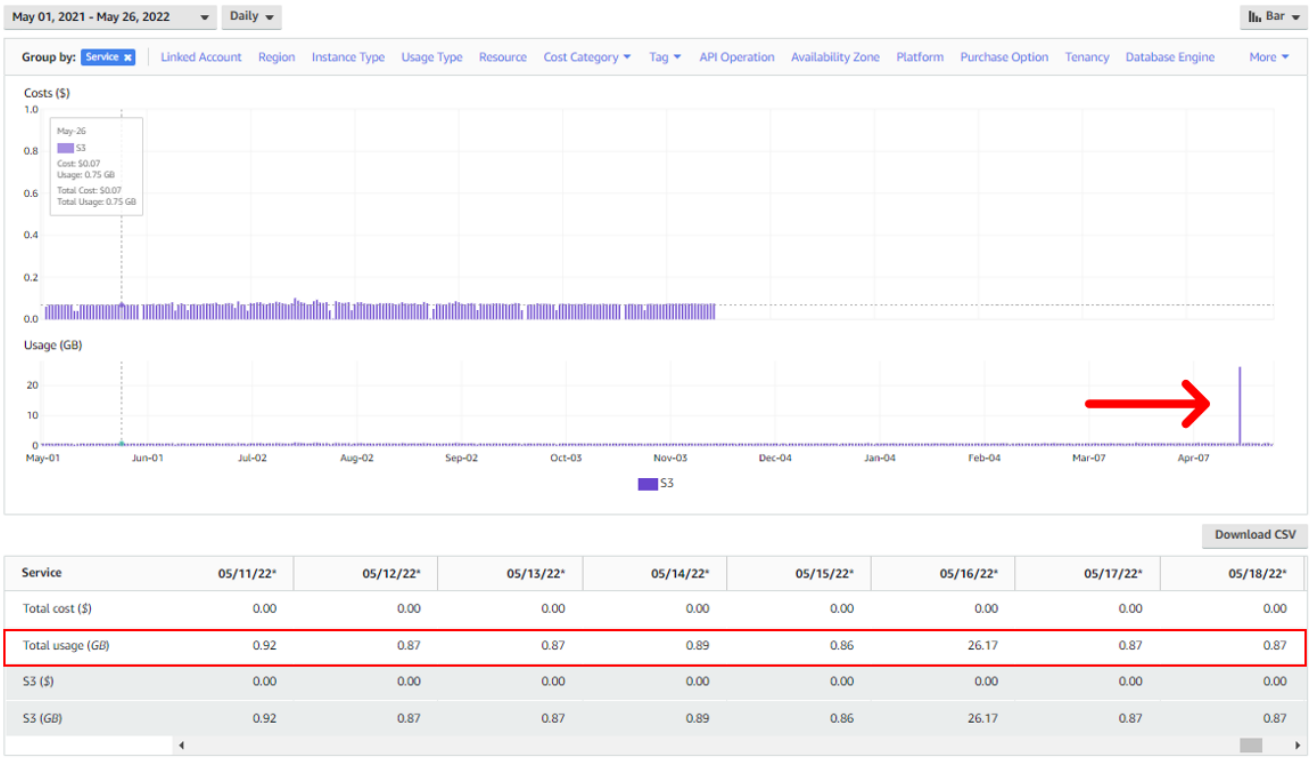


Figure 6. Cost Explorer filtered on API Operation

The bottom arrows in Figure 6 above indicate that the 300 GB worth of data was transferred using the “GetObject” API call, which is again a clear anomaly based on the other 6 months of historical “GetObject” usage. While Cost Explorer will not provide information regarding what specific objects were downloaded, a forensic investigator now has a more definitive time frame to conduct further investigation.

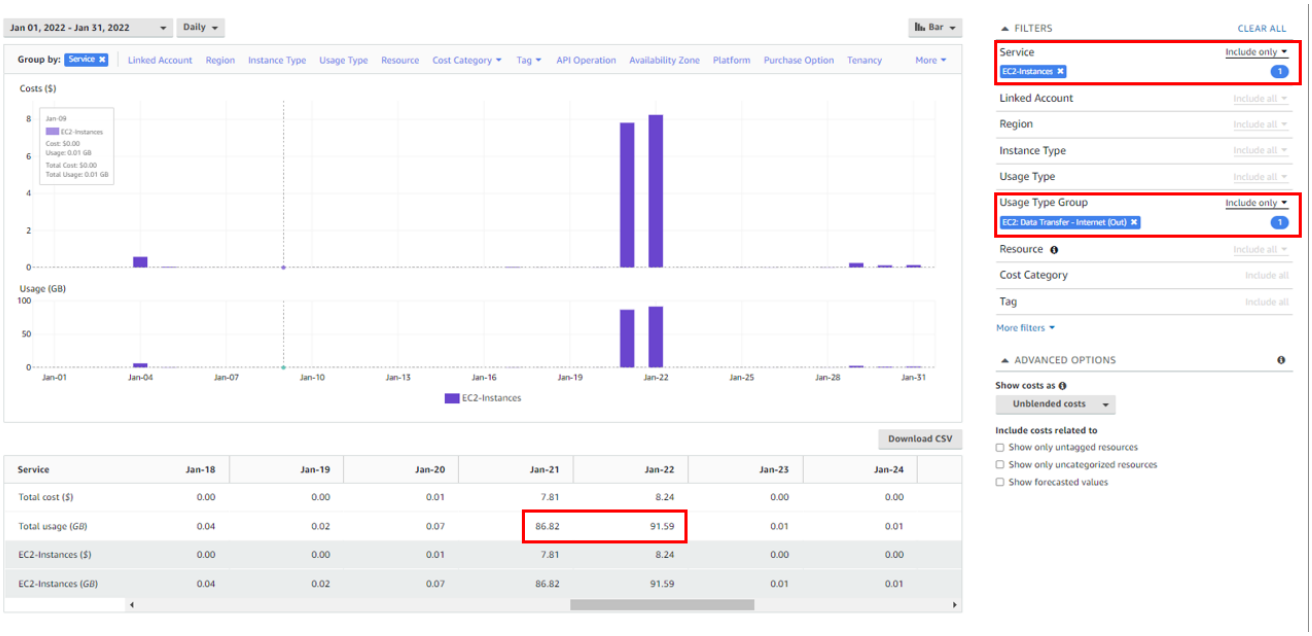
Stroz Friedberg used this same methodology to determine if data from an unintended publicly accessible AWS S3 bucket was exfiltrated. Review of the Cost Explorer Usage graph (Figure 7) revealed a spike in data transfer on May 16, 2022. On this date, 26.17 GB worth of data was transferred out to the internet. Compare this with the average daily transfer rate of just under 1 GB over the last 12 months, and it was clear that May 16, 2022 was a date of interest. While granular object-level logging was not enabled on this particular AWS S3 bucket to investigate further, the bucket size was just over 26 GB. Using this, Stroz Friedberg was able to make a reasonable inference that all objects in this AWS S3 bucket were likely exfiltrated.



Service	05/11/22*	05/12/22*	05/13/22*	05/14/22*	05/15/22*	05/16/22*	05/17/22*	05/18/22*
Total cost ($)	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Total usage (GB)	0.92	0.87	0.87	0.89	0.86	26.17	0.87	0.87
S3 ($)	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
S3 (GB)	0.92	0.87	0.87	0.89	0.86	26.17	0.87	0.87

Figure 7. Another example of a large outbound data transfer spike in AWS S3

The same methodology can be applied for other AWS services such as Elastic Compute Cloud (“EC2”) (shown in Figure 8) and Relational Database Service (“RDS”).



Service	Jan-18	Jan-19	Jan-20	Jan-21	Jan-22	Jan-23	Jan-24
Total cost ($)	0.00	0.00	0.01	7.81	8.24	0.00	0.00
Total usage (GB)	0.04	0.02	0.07	86.82	91.59	0.01	0.01
EC2-Instances ($)	0.00	0.00	0.01	7.81	8.24	0.00	0.00
EC2-Instances (GB)	0.04	0.02	0.07	86.82	91.59	0.01	0.01

Figure 8. Cost Explorer detailing an anomalous external data transfer in the EC2 service on January 21 and 22, 2022

Additional Use Cases for AWS Cost Explorer

Validating Threat Actor Exfiltration Claims

In matters involving unauthorized access to data within AWS, it is not uncommon for a threat actor to attempt to extort the affected organization. Stroz Friedberg has seen this firsthand, especially with regards to AWS S3 and RDS services. Cost Explorer can be used to validate a threat actor's claim of data exfiltration. For instance, if the threat actor claims to have exfiltrated 250 GB worth of data from AWS S3 and Cost Explorer shows a data transfer approximately 250 GB in size around the time of interest that is unaccounted for in legitimate business activity, the company can infer that the threat actor likely has that volume of data and can approach interactions with the threat actor accordingly.

Identifying Anomalous Service Usage

AWS administrators may find regularly checking Cost Explorer each month useful for identifying anomalous behavior such as new service usage. For example, if your organization does not use AWS's Route 53 DNS ("Domain Name System") service, then sudden usage of this service may indicate a threat actor using the environment for hosting command and control ("C2") infrastructure.

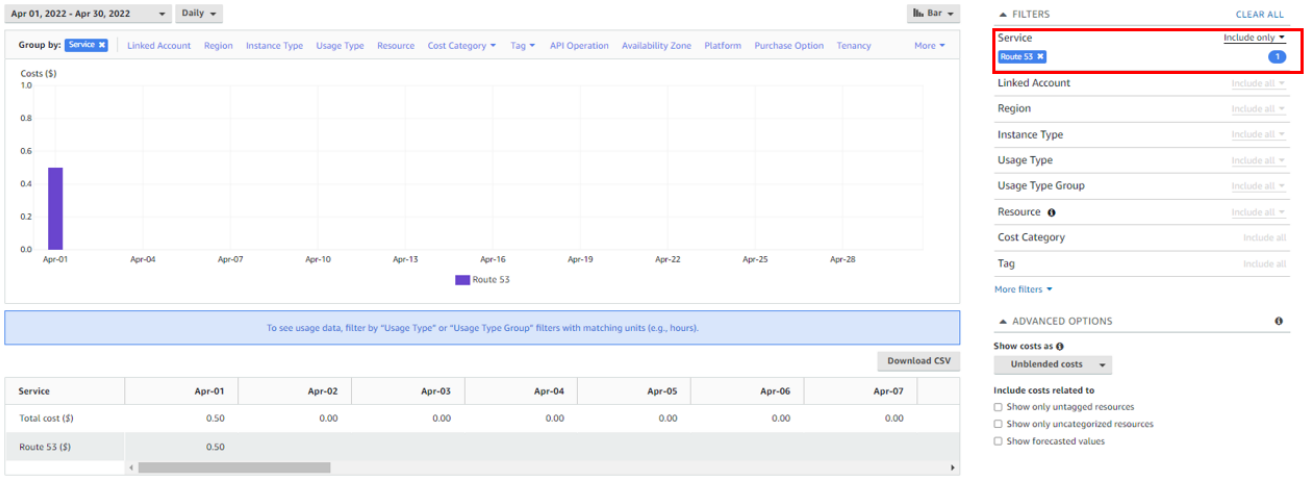


Figure 9. Cost Explorer filtered on Route 53 service

Another example of anomalous service usage may be a spike in AWS Lambda activity. Lambda is a serverless computing platform that can run code for virtually any type of application. Threat actors have increasingly targeted Lambda to run code associated with mining cryptocurrency.

Identifying New Region Usage

A common technique threat actors use to evade detection when compromising an AWS environment, is to spin up resources in an AWS region that is not being used. Cost Explorer can help detect suspicious new region usage by simply applying “Region” to the Group by feature within the Cost Explorer visualization tool.

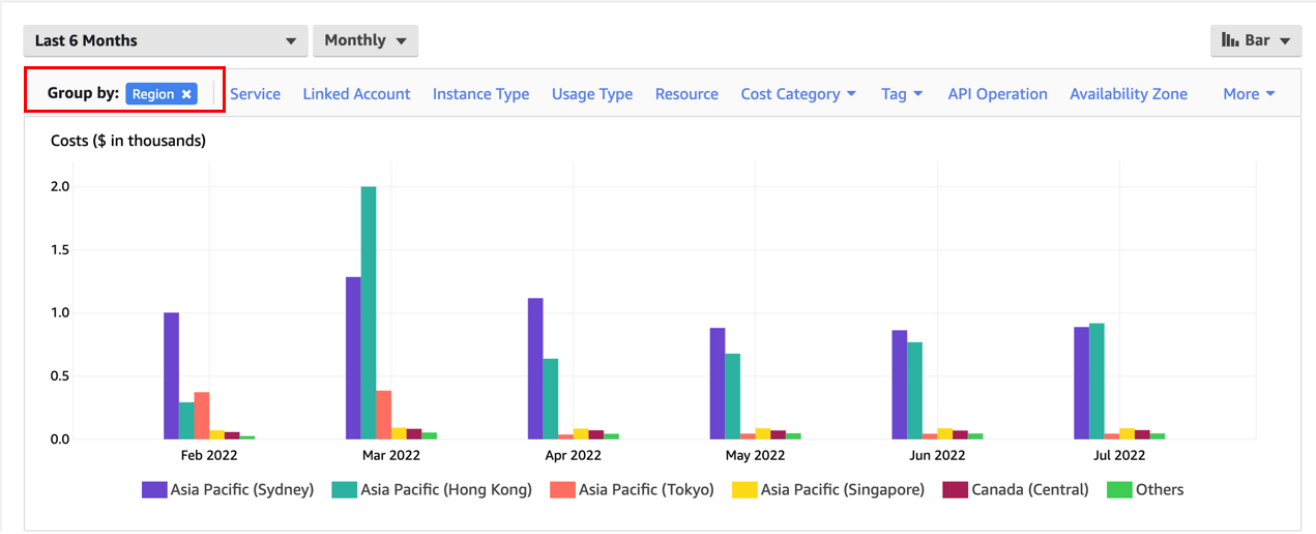


Figure 10. Cost Explorer grouped by “Region”

AWS Cost Explorer Limitations

While AWS Cost Explorer can be very useful, it is important to understand its limitations and gaps. For one, cost metrics within Cost Explorer may be affected by free tier service usage, volume-based discounts, reserved instance contracts, and services which are billed monthly or annually. Additionally, Cost Explorer may take up to 24 hours to reflect costs. As such, it is

not a valid tool or replacement for real time monitoring of an AWS environment. For real time cost anomaly analysis and alerting, one may consider using AWS's Cost Anomaly Detection service.

Conclusion

Stroz Friedberg continues to see an increase in the number of investigations that involve cloud services such as Amazon Web Services. Digital forensics often involves leveraging existing artifacts and data in creative and innovative ways, viewing them from a different perspective from what they were intended for to solve often-complex matters. In that vein, AWS Cost Explorer has resulted in many quick wins for Stroz Friedberg's investigators, and it is a valuable data point that can be leveraged to look for anomalous activity within your own AWS environment or fill in gaps in an investigation of such an environment. If you are seeing anomalous behavior in your AWS environment Stroz Friedberg's team of experienced investigators can help determine the scope and root cause of the activity.

Author: Andre Maccarone, John Ailes
Special Thanks: Chapin Bryce
October 6, 2022

Cyber security services offered by Stroz Friedberg Inc. and its affiliates. Insurance products and services offered by Aon Risk Insurance Services West, Inc., Aon Risk Services Central, Inc., Aon Risk Services Northeast, Inc., Aon Risk Services Southwest, Inc., and Aon Risk Services, Inc. of Florida and their licensed affiliates. Aon UK Limited is authorised and regulated by the Financial Conduct Authority in respect of insurance distribution services. FP.AGRC.238.JJ The following products or services are not regulated by the Financial Conduct Authority:

- Cyber risk services provided by Aon UK Limited and its affiliates
- Cyber security services provided by Stroz Friedberg Limited and its affiliates.