The Rise of S3 Ransomware

In today's digital landscape, around 60% of corporate data now resides in the cloud, with Amazon S3 standing as the backbone of data storage for many major corporations.

Despite S3 being a secure service from a reputable provider, its pivotal role in handling vast amounts of sensitive data (customer personal information, financial data, intellectual property, etc.), provides a juicy target for threat actors. It remains susceptible to ransomware attacks which are often initiated using leaked access keys that have accidentally been exposed by human error and have access to the organization's buckets.

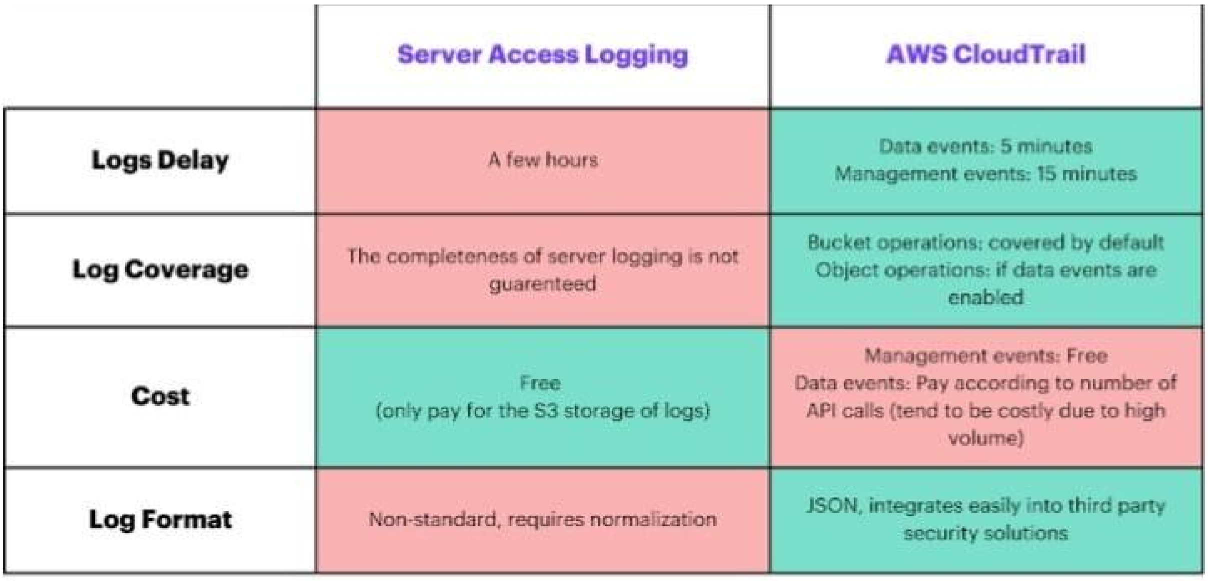
To effectively combat these evolving threats, it is vital to ensure that your organization has visibility into your S3 environment, that you are aware of how threat actors can compromise data for ransom and most importantly, best practices for minimizing the risk of cyber criminals successfully executing such an attack.

Ensuring Visibility: CloudTrail and Server Access Logs

Visibility serves as the foundation for any effective detection strategy. In Amazon S3, nearly every action translates to an API call, which are meticulously recorded in CloudTrail and documented in AWS documentation.

The two primary options for logging activity in S3 buckets — CloudTrail Data Events and Server Access Logs — hold a wealth of information that security practitioners must leverage to anticipate and detect suspicious activity. Each offer distinct advantages and trade-offs:

- Cloud Trail Data Events: offer visibility into resource operations performed on or within a resource in real-time, but comes with potential cost implications due to high API call volumes
- Server Access Logs: free access to records for each request made to your S3 bucket, but come with potential delays in log availability and potential logging with less integrity.



	Server Access Logging	AWS CloudTrail
Logs Delay	A few hours	Data events: 5 minutes Management events: 15 minutes
Log Coverage	The completeness of server logging is not guarenteed	Bucket operations: covered by default Object operations: if data events are enabled
Cost	Free (only pay for the S3 storage of logs)	Management events: Free Data events: Pay according to number of API calls (tend to be costly due to high volume)
Log Format	Non-standard, requires normalization	JSON, integrates easily into third party security solutions

The advantages and trade-offs between Server Access Logs and AWS CloudTrial logs.

Mitigating Risk by Understanding the Attack Scenarios

Utilizing the above logs to ensure adequate visibility, it is possible to keep an eye out for potential attack scenarios in order to mitigate risks effectively. There are three main attack scenarios that we observe with S3 ransomware attacks, all which can prevent an organization from accessing its data. Below are the attack scenarios, along with links to hunting queries that the expert threat hunting team from Hunters' Team Axon has shared publicly that allow anyone to search for these attack scenarios within their own environments:

1. Object Encryption: ransomware commonly involves file encryption to deny an organization access to their files, harm business operations and demand ransom for getting the files back
2. Object Deletion - Delete Operations: deleting all objects from a bucket is an easy way for threat actors to have a major impact on business operations, improving the chances of victims paying ransoms

3. Object Deletion - Lifecycle Policy: a less straightforward but quieter way to delete files in Cloudtrail that still offers high chances of a paid ransom

**Note: Object Encryption and Object Deletion - Delete Operations require enabling Cloudtrail Data Events for the appropriate buckets.*

Each scenario poses significant disruptions, potentially preventing organizations from accessing critical data. By delving into the required permissions, attacker perspectives, and detection methods for each scenario, organizations can proactively prepare for potential threats.

Protection and Best Practices

Understanding the attack scenarios helps to provide context for how to implement proactive measures to significantly reduce the attack surface. There are several things that can be done to enhance the security of S3 buckets from the threat of ransomware.

- Use IAM roles for short-term credentials: avoid using static IAM access keys. If you are using IAM users, be sure to enable Multi-Factor Authentication (MFA) for them.
- Follow the principle of least privilege: this ensures that users and roles only possess the permissions necessary for their tasks. Additionally, utilize bucket policies to restrict access to these essential resources.
- Enable S3 Versioning: this means keeping record of every version of every object stored in your bucket instead of directly modifying it. This is very effective against unauthorized override or deletions.
- Enable S3 Object Lock: operating on a write-once, read-many (WORM) model, means that your data cannot be deleted by anyone (the data is "locked") which safeguards against modifications for defined time periods.
- Set up AWS Backup/Bucket Replication: this can be any form of backup that is separate in location and access control from your actual bucket.
- Implement server-side encryption with AWS KMS keys: this provides your organization with specific control over who can

access bucket objects. This supplies yet another level of protection against who can encrypt and decrypt objects in your bucket.

Conclusion

As data volumes continue to surge, securing Amazon S3 is paramount in safeguarding millions of organizations against ransomware attacks and evolving cyber threats.

Prioritizing threats, ensuring visibility through CloudTrail and Server Access Logs, and implementing proactive measures are essential steps in mitigating risk. By adopting these strategies, organizations can fortify their S3 buckets' protection and ensure the integrity and security of their critical data.

Author - Himangshu Sarkar

Github - https://github.com/Himangshu30

LinkedIN - https://www.linkedin.com/in/himangshu-sarkar-b4ba3a22a