

Mitigating S3 bucket Ransomware with AltorCloud

Amazon S3 buckets are widely used by organizations to store and share data in the cloud. However, these buckets are also potential targets for ransomware attacks. Ransomware is malware that encrypts or deletes data on a victim's system and demands a ransom payment in exchange for the decryption key. This white paper discusses the threat of S3 bucket ransomware attacks and provides guidance on how organizations can protect their S3 buckets from these attacks.



Background:

Amazon S3 (Simple Storage Service) is a robust cloudbased static file storage service offered by Amazon Web Services (AWS). It provides organizations with a simple and scalable way to store and retrieve data in the cloud. S3 buckets store a wide variety of data, including files, images, videos, and backups. While S3 buckets are highly useful for businesses, they also represent a potential target for attackers.



S3 Ransomware Attack Vector:

Attackers can gain access to S3 buckets using various attack vectors. Phishing attacks, where attackers trick victims into revealing their login credentials, are among the most common attack vectors. Attackers can also exploit vulnerabilities in third-party software used by the organization to gain access to S3 buckets.

Once an attacker gains access to an S3 bucket, they can proceed to encrypt or delete the data in the bucket and demand a ransom payment in exchange for the decryption key. S3 ransomware attacks can have severe consequences for organizations, as data loss can lead to financial loss, reputational damage, and legal liability.

Real-World Example:

In 2021, a major insurance company was hit by an S3 ransomware attack. The attackers used a phishing email to gain access to the company's S3 bucket and then proceeded to encrypt all the files in the bucket. The attackers then demanded a ransom payment in Bitcoin in exchange for the decryption key. The company had to pay a ransom to recover their data.



Protecting Against S3 Ransomware Attacks:

Organizations can take several steps to protect their S3 buckets from ransomware attacks. These include:

- Strong Passwords and Multi-Factor Authentication: Organizations should use strong passwords and enable multi-factor authentication for all S3 bucket users. This can help prevent attackers from gaining unauthorized access to S3 buckets.
- Restrict Access: Organizations should restrict S3 buckets to only authorized users. This can be achieved by using AWS Identity and Access Management (IAM) policies to control access to S3 buckets.
- Monitor Access Logs: Organizations should monitor access logs for S3 buckets to detect suspicious activity. They should also enable AWS CloudTrail to log all S3 bucket activity.
- Versioning and Backups: Organizations should use versioning and backups to protect against data loss. Versioning allows organizations to recover previous versions of a file, while backups can be used to restore data in the event of a ransomware attack.

As the use of Amazon S3 buckets continues to increase, so does the threat of ransomware attacks targeting these buckets.



Prevention Measures:

- Implement Security Best Practices: Organizations should implement security best practices, such as using strong passwords, enabling multi-factor authentication, and restricting access to S3 buckets to only authorized users. They should also regularly review and update their security policies and procedures.
- Conduct Regular Security Audits: Organizations should conduct regular security audits to identify vulnerabilities in their S3 buckets. These audits can include vulnerability scans, penetration testing, and security assessments leveraging AltorCloud.
- Educate Users: Organizations should educate their users on recognizing and reporting suspicious activity. This can include phishing emails, unauthorized access attempts, and unusual file deletions.
- Use Data Encryption: Organizations should use data encryption to protect their data in transit and at rest. This can help prevent attackers from accessing and stealing sensitive data.



Defense Measures:

- Monitor Access Logs: Organizations should monitor access logs for S3 buckets to detect and respond to suspicious activity. They should also enable AWS CloudTrail to log all S3 bucket activity.
- Leverage a CSPM (Cloud Security Posture Management) tool to perform regular assessments and continuous monitoring of configurations to identify misconfigurations that can lead to a data breach. AltorCloud can generate compliance reports demonstrating adherence to security best practices, such as enabling object versioning and MFA delete.
- Implement File Versioning: Organizations should implement file versioning for their S3 buckets. This can help protect against data loss by allowing users to recover previous versions of a file. AltorCloud can remediate misconfigurations by providing policy-based rules. For example, If an S3 bucket is found to have MFA delete disabled, the tool can provide you with manual remediation steps, scripts, and templates to resolve the misconfiguration.
- Use Data Backups: Organizations should use data backups to protect against data loss in the event of a ransomware attack. Backups should be stored in a secure, off-site location and regularly tested for integrity and reliability.
- Implement Disaster Recovery Plans: Organizations should implement disaster recovery plans that include procedures for responding to ransomware attacks. These plans should be regularly tested and updated to ensure they are effective.



How to detect S3 bucket ransomware misconfigurations leveraging AltorCloud

1. Log into your AltorCloud account

AltorCloud	
🖾 Email	AltorCloud
Password	AlterCloud provides security teams with real-time visibility into your organization's security posture with compliance reporting,
Remember me Forget your Pessword? LOCIN Need on account?*= Sign Up Problems verifying email? = Seend verification	risk assessments and actionable intelligence
emot	

2. Once you log in, you will see your AltorCloud dashboard. Navigate to results and Aws findings.

No. Const.	DASHBOARD SCAN RESULTS + INVENTORY + REPORT ADMIN	weights - Advert
Dashboard		
619 M 8		Contornin Depherond
3 Accounts 😁 🛆 🛆	137 Total Findings	Tensor cheloss ar proventer fabilian ten Deste AAN
март алтаства рокшие ит сонтила. назва В 627 429	AD. WE RECOMPLETE POWER REPORT OF THE POWER REPORT OF THE POWER REPORT OF THE POWER REPORT.	Next Maker Nat Calific Visite
	Interfaces (20). South LBK	AND REDUKCE OVERVEX
en Doudral	tic) workers i worker i worker Datar-Poy Edatariekou och	O
20	Davlor-Cr.+Matter-Updated -Set25cectemorethil Coet10 ped 443	View ABIS Securities
CCP RESOURCES CONTINUES File contraction for a data Real is accon	10-logitoth (-oxiduationation) VereitCE Instances	top balans (mix nations Check/IIS securics memorystal ddd
	COMPLIANCE CONTROLS PASSED BY ELANDARD	📇 Ensure there are no Security Croupe not being used. 🛛
	😸 CD-ANS 💼 📩 🙀 🙀 🙀	Einzerbreis der of Soczity Orouge ettraut ingese Riemitg being und SO Einzerbreis der of Soczity Orouge ettraut ingese Riemitg being und SO Einzerbreis der of Soczity Orouge ettraut ingese Riemitg being und SO Orouge Hill burder Mit Dateite sind erweisel SO
	x - 5%	
AltorCloud	DASHBOARD SCAN RESULT	S - INVENTORY - REPORT ADMIN
Dashboard	AZURE	



3. You can view all your risk totals from the AWS security results page. Click on the Findings button.



4. On the AWS security results page, you can filter by Compliance controls such as CIS, HIPAA, PCI-DSS, etc., Checks passed, failed, disabled, and Risk – Critical, high, medium, and low. For this example, we will search for the service S3.

Security Res	Ults AWECHICK	S OVERVEN	W FINDINGS					
OUN FI	SCAN: Tue, 28 Fe	6 2023 18:27:35	GMT 8					Remediate Finde
OW 10 & ENTRIES	Filter (failed) +				SEARCH:	s3 O	Check \$3 Account Level Public Access Block.	
	CHECKS © Foiled	RISK	net	· 8:54	 COMPLIANCE 	FAILURES ()	CIS-AWS v1.5: 2.1.5, HIPAA: 164_308_0_1, IL-b, HIPAA: 164_308_0_3, I	
PHECK 53 R ODPR	O Passed O Remediable	M High		High	CIS-ANS VIS 215 HIPAA 164_308_0_1_8_b.	1	Risk & Remediation Evidence Extra Info	
neure 53 PCI-DSS 3 bucket	O DISOBIED	LOW .	(Tropil	Medium	CIS-AWS VL5: 3.6 GORE article_25	π	RISK & REMEDIATION	Ed
nsune o li- honges.	Apply		Nench	Medium	CIS-AWS VIS 4.8 ODPR orticle_25	1	RISK DESCRIPTION	
heck if \$3 buckets have A	ts enobled	53		Medium		84	REMEDIATION	
heck #53 buckets have de se a bucket policy to enfor	rlault encryption (656) en ce it	abled or \$3		Medium	CIS-AWS VIS 213 GORE onticle_32	3	*** utilizing Block Public Access (bucket settings)**	
heck #53 bucket MFA Dele	te is not enabled.	\$3		Medium	CIS-AWS vI.5: 23.3	92	From Console	
heck if \$3 buckets have of	iject versioning enobled	53		Medium	1673.A) 364_308_0_1_8_0 1673.A 364_308_0_7_L	84	E login to AWS Management Console and open the Amazon S3 console using https://console.aws.amazon.com/s3/ 2. Select the Check bar next to the Bucket.	
heck if \$3 buckets have se	cure transport policy.	\$3		Medium	Cri-AWS v15 212 0099: orticle_32	92	Click on Totil public access settings: A. Cick Block of public access Settings Separate for all public access Separate for all the buckets in your AWS account that contain sensitive data.	
heck il 53 buckets have se	rver access logging enab	pled \$3		Medium	HPAA. 164_308_0_1_8_d 167AA: 164_308_0_3_8_0_	88	Frem Command Line L just all of the S3 Buckets	
heck if \$3 buckets have 0 enabled in CloudTrail.	bject-level logging for rea	ad events Clo	ind Trail	Low	CIS-AWS VLS 33 OCPR onticle_30_	1	coves s3 is	



5. Identify the S3 bucket misconfigurations that need to be resolved. For this whitepaper, we want to fix three misconfigurations.

a.Check S3 account level Public Access Block.

b.Check S3 Bucket MFA delete is not enabled.

c.Check S3 buckets have object versioning enabled.

NAME	1	SERVICE	0	RIS	i K	*	COMPLIANCE	FAILURES	0	0
Check S3 Account Level Public Access Block.		\$3		High			CIS-AWS v1.5: 2.1.5 HIPAA: 164_308_0_1_ii_b_		1	
Check if \$3 bucket MFA Delete is not enabled.		\$3		Mediun	m		CIS-AWS v1.5: 2.1.3		92	
Check if \$3 buckets have object versioning enabled		\$3		Mediun	m		HIPAA: 164_308_a_1_ii_b HIPAA: 164_308_a_7_i_		84	

We can see how many failures each check has.

6. Let's check which S3 buckets are misconfigured. Click on the Evidence tab next to Risk and Remediation.

SCAN: Tue, 28 Feb 2023 18:2	17:35 GMT #							Remediate Finding
IOW 10 & LATERS Filter (Faled) +			S(ARCH	ы О	Check If 53 bucket MFA De	lete is not enabled.		
NAME	SERVICE	RISK	- COMPLIANCE	FAILURES ()	CI5-AWS-VI.5: 2.1.3			
Check 53 Account Level Public Access Block.	53	High	CIS-AWS VLS 215 HPAA:	1	Risk & Remediation	Evidence Extra Info		
nsure 53 bucket access logging is enabled on the Cloud?rail 3 bucket	CloudTrail	Medium	CIS-AWS VIS 3.6 GOPR onticle_25	17	92 FAILURES			Copy Evidence
nsure a log metric filter and alarm exist for 53 bucket policy hanges.	CloudWatch	Medium	CIS-AV45 v15 48 00PR orticle_25	ï	REBOURCE		* REGION	
Theck if 53 buckets have ACLs enabled	13	Medium		84	ossets		us-west-1	
Check if \$3 buckets have default encryption (\$55) enabled or use a bucket policy to enforce it.	13	Medium	CIS-AWS VLS 213 COPR orSole_32.	3	ndcom	39395423-us-west-2	us-eest-1	
Theck if \$3 bucket MFA Delete is not enabled.	13	Macham	CIS-AWS vLS 213	92		'ec/9278	so-east-1	
Theck if 53 buckets have object versioning enabled	ទា	Medium	HEPAA:	84		oeldde	sa-east-1	
			164_308_0_1_8_5 HPAA: 164_308_0_7_1_			215106	us-west-2	
Sheck if \$3 buckets have secure transport policy.	53	Medium	CIS-AWS VIS 212	92		942453	tor-east-1	
	213	_	GIOPR onticle_32	200		71c851	1-tase-east	
Check if 53 buckets have server access logging enabled 53	53	Medium	164_308_0_1_II_d			357+918	sa-east-1	
			HPAA. HH4_308_0_3_8_0			x646c4f	sa-east-1	
Check if 53 buckets have Object-level logging for read events	CloudTrail	Low	CIS-AWS VLS: 3.8	1		8-05-0-05	us-west-2	
is enabled in CloudTrail.			GOPR onticle_30.			2056203	sa-east-1	
						14d4c8d	sis-west-2	



7. We now have the resources that need remediation. AltorCloud provides remediation information so the issue can be remediated. We also offer Terraform and cloud formation templates that can be leveraged to remediate misconfigurations.

HOW 10 # ENTRIES Fater (Falled) *			SEARCH:	s3	0	
NAME	SERVICE +	BISK +	COMPLIANCE	FAILURES ()		GIS-AWS VI.5: 2.1.3
Check 33 Account Level Public Access Block.	53	High	CIS-AWS VLS 23.5 HIPAA 164_308_0_1_8_8.	Ť.		Risk & Remediation Evidence Extra Info
Ensure \$3 bucket access logging is enabled on the CloudFrail \$3 bucket	Cloudfroll	Medlum	CIS-AWS VLS: 3.6 GOPP: prticle_25	12		RISK & REMEDIATION
Ensure a log metric filter and alarm exist for 53 bucket policy changes.	CloudWatch	Medium	CIS-AWS VEB: 4.8 GOPR onScie_25	1		RESK DESCRIPTION Your security credentials are compromised or unauthorized access is granted.
Check if S3 buckets have ACLs enabled	53	Medium		84		REMEDIATION
Check if 53 buckets have default encryption (55E) enabled or use a bucket policy to enforce it;	50	Medium	CIS-AWS VES 218 GOPR orticle_32.	3		Perform the steps below to enable MFA delete on an 53 bucket.
Check If 53 bucket MFA Delete is not enabled.	13	Medium	CIS-AWS vi 5: 213	92		Note: - You prevent excition MEA Datate using the 20th Management Constale. You must use the 30th C11 or API
Check if \$3 buckets have object versioning enabled	\$3	Medium	HPAA: 164_308_0_1_8_b HPAA: 164_308_0_7_k.	84		*You must use your hoof account to enable MFA Delete on S3 buckets. **from Commond line**
Check if 53 buckets have secure transport policy.	50	Medium	CIS-AWS vills 212 GOPR orticle_12_	92		1. Run the s3opi put-bucket-versioning command
Check if 53 buckets have server access logging enabled	93 -	Medium	HPAA: 184_308_0_1_i_d HPAA: 184_308_0_3_i_0.	88		
Check if 53 buckets have Object-level logging for read events is enabled in CloudTrail.	CloudTrail	Low	CIS-AWS VLS: 3.8 GORR onticle_30	1		REFERENCE
HOWING I TO TO OF IT ENTRIES (FILTERED FROM 166 TOTAL ENT	N(S)					https://docs.aws.amazon.com/Amazon531/latest/userguide/MultiFactorAuthenticationDelete.html

8. Once remediated, scan your environment and ensure all traces of the misconfiguration are gone.



Conclusion:

S3 ransomware attacks are a growing threat to organizations using Amazon S3 buckets. These attacks can have severe consequences, including financial loss, reputational damage, and legal liability. Organizations can protect their S3 buckets from ransomware attacks by implementing prevention and defense measures, such as deploying a cloud security posture management tool like AltorCloud. Implementing security best practices, conducting regular security audits, educating users, using data encryption, monitoring access logs, implementing file versioning, using data backups, and implementing disaster recovery plans. By taking these steps, organizations can reduce the risk of an S3 ransomware attack and protect their valuable data in the cloud.



AltorCloud



www.altorcloud.com



@altor_cloud



altorcloud