deep instinct

Threat Landscape Report

Special Edition: Amazon Simple Storage Service (S3)

DEEP INSTINCT THREAT LAB

March 2024

Table of Contents

Authors

MARK VAITZMAN
Threat Lab Team Leader

SIMON KENIN
Threat Intelligence Researcher

IVAN KOSAREV
Threat Intelligence Researcher

Executive Summary

Cloud storage has become the go-to solution for businesses of all sizes, offering scalability, cost-effectiveness, and accessibility. According to Research and Markets the global cloud storage market grew from **$83.55 billion in 2022 to $100.2 billion in 2023** at a CAGR of 19.9% (it was just $40 billion in 2020).

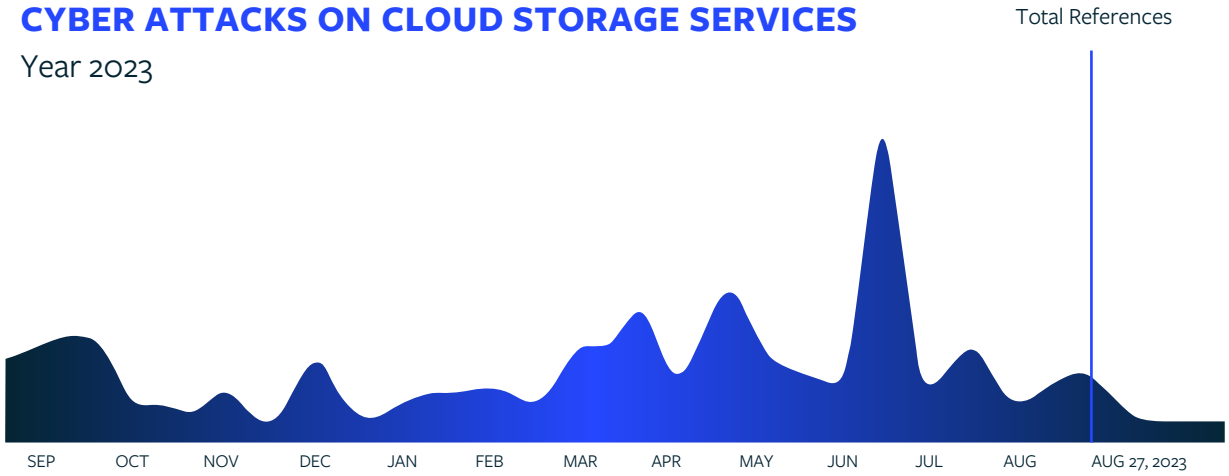
Enterprises are increasingly turning to cloud storage to reduce costs and improve operational efficiency. However, as digitalization has taken on a new priority, **the threats related to cloud security have also increased the attack surface**, making cloud storage, particularly S3 buckets in AWS, a prime target for cybercriminals.

This report analyzes the current cloud storage security landscape, with a particular focus on the AWS S3 threat landscape, highlighting recent cyberattacks, evolving MITRE techniques, threat actors, impacts, and best practices for securing your data.

Driving Factors for Cloud Storage Growth

CYBER ATTACKS ON CLOUD STORAGE SERVICES

Year 2023



The rapid growth of cloud storage adoption in recent years can be attributed to several key trends and benefits:

- **Explosion of data:** Global data generation is increasing exponentially, from 2 zettabytes in 2015 to an estimated 181 zettabytes in 2025. This demand for storage drives cloud adoption.
- **Remote work and digital transformation:** The pandemic accelerated the shift towards remote work and cloud-based services, further bolstering cloud storage usage.
- **Cost-effectiveness:** Cloud storage offers flexible and scalable storage options at competitive costs compared to traditional on-premises infrastructure.
- **Accessibility and collaboration:** Cloud storage facilitates remote access and collaboration on data, increasing its appeal for businesses and individuals.

LOOKING AHEAD

The cloud storage market is expected to continue its strong growth trajectory in the coming years, with estimates suggesting it could reach over

$370 BILLION

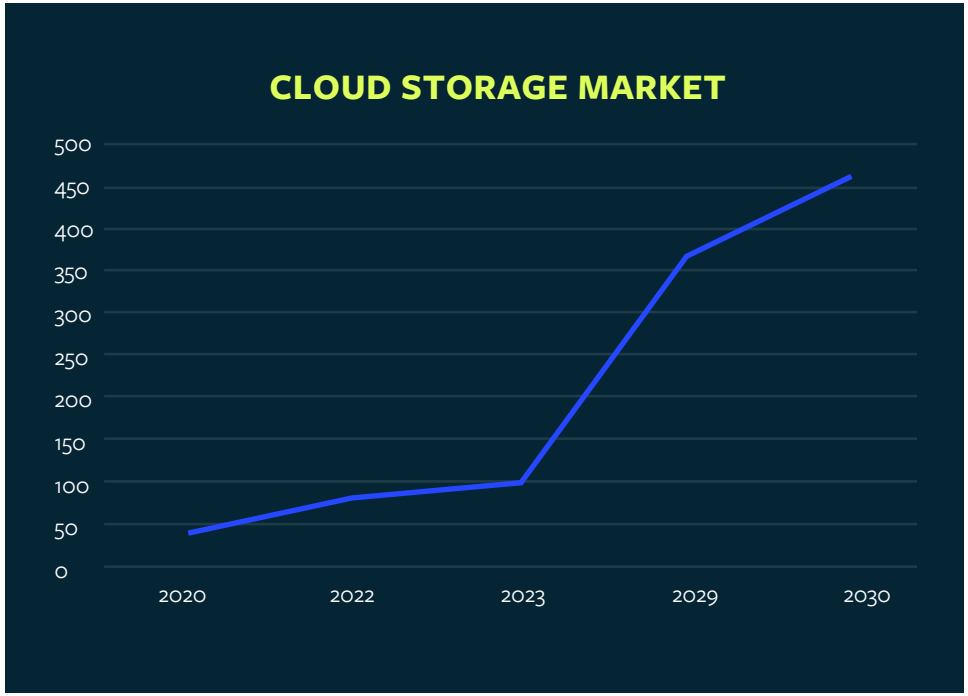
by 2029

New technologies like multi-cloud adoption and AI-powered data management are expected to shape the landscape further.

MITRE ATT&CK Framework

As cloud storage becomes ubiquitous, attackers are evolving MITRE techniques to exploit misconfigured S3 buckets and other publicly accessible data repositories. Here are the primary evolving MITRE techniques in cloud storage:

- **Reconnaissance (RECON):** Attackers scan for open S3 buckets using automated tools and exploit search engines to identify buckets with publicly accessible data.
- **Resource Hijacking (RHIJ):** Unrestricted access to S3 buckets allows attackers to mine cryptocurrency, launch DDoS attacks, or host malware in the cloud.
- **Lateral Movement (LATERAL):** Access to one S3 bucket can be used as a foothold to pivot and compromise other cloud resources within the AWS environment.
- **Command and Control (C2):** Attackers can store malicious scripts or executables in S3 buckets and use them to control compromised systems.



Trends

Attackers are exploiting new vulnerabilities and attack vectors to compromise data stored in services like Amazon S3. Some key trends shaping the threat landscape include:

- **Increased automation:** Attackers increasingly use automated tools and scripts to identify and exploit vulnerable S3 buckets.
- **Focus on data exfiltration:** Stealing sensitive data remains the primary objective for attackers, who often target specific file types containing personally identifiable information (PII) or financial information. Underground marketplaces offer tools and services for stealing data from cloud storage and potentially exposed cloud storage lists, including S3 buckets.
- **Multi-stage attacks:** Attackers are combining multiple MITRE techniques to launch sophisticated attacks that evade detection and maximize impact.
- **Supply chain attacks:** Targeting third-party applications or services integrated with S3 buckets opens new attack vectors as cloud storage provides integrated software markets.
- **Cloud-native attacks:** Exploiting specific cloud functionalities and APIs to compromise S3 buckets are becoming more sophisticated.
- **Ransomware:** Encrypting data stored in S3 buckets and demanding ransom payments is a growing threat.
- **Phishing and social engineering:** Targeted attacks are becoming more sophisticated, tricking users into revealing credentials or granting access.
- **Containerized attacks:** Exploiting vulnerabilities in container technology used for microservices deployment in cloud environments.

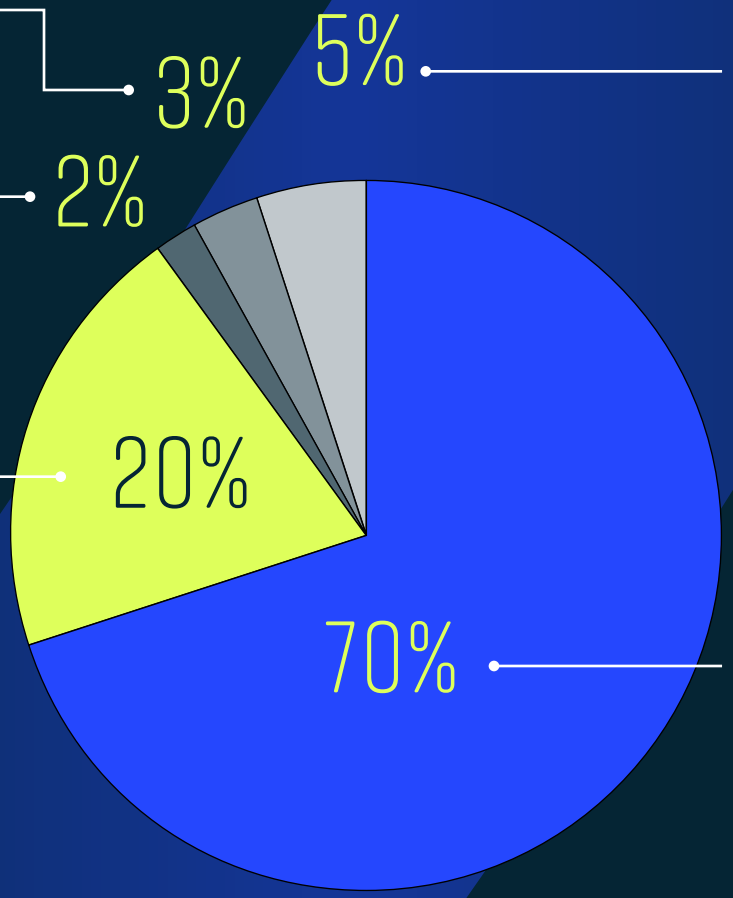
Threat Landscape and Vulnerabilities

The cloud storage threat landscape encompasses a range of attack vectors that take advantage of misconfigurations, vulnerabilities, and other weaknesses to compromise data. Based on recent analyses, the most common issues enabling attacks include:

Supply chain attacks (3%): Compromised third-party applications or services connected to cloud storage pose a growing threat.

Advanced persistent threats (APTs) (2%): Targeted attacks by nation-state actors and sophisticated criminal organizations occur less frequently but can have significant consequences.

Data breaches (20%): Insider threats, social engineering, and vulnerabilities in cloud services contribute to approximately 20% of attacks, leading to data exposure.



Ransomware attacks (5%): While still in its early stages, ransomware targeting cloud storage is rising, accounting for roughly 5% of recent attacks.

Misconfigurations (70%): Improper access controls, outdated software, and open buckets remain the most frequent vulnerabilities, occurring in about 70% of cloud storage attacks.

CLOUD STORAGE THREAT LANDSCAPE

Malware Execution

S3 buckets are primarily designed for storage, not execution. While some limited execution capabilities exist, their functionality is restricted and unlikely to support complex malware detonation. But if an S3 bucket is misconfigured with open access or insufficient access controls, a threat actor could upload and execute malware within the bucket itself. This could involve scripting languages like Python or JavaScript, which AWS Lambda supports. Exploiting vulnerabilities in server-side code associated with the S3 bucket could also allow an attacker to inject malicious code and execute it within the bucket's environment.

Modern cloud providers typically implement security measures and sandboxing that can limit the impact of malicious code execution within their environments. This could restrict the malware's ability to spread or access sensitive data.

Malware Distribution

Malware distribution in cloud storage includes various techniques attackers employ to spread malicious software through platforms like Amazon S3, Microsoft Azure Blob Storage, and Google Cloud Storage. The following are the most common malware types:

CRYPTOJACKING MALWARE (50-60%):

- Driven by financial gain, cryptojacking remains a prominent threat, often leveraging misconfigured cloud servers and container environments to deploy mining scripts (SIA, for example).
- Studies suggest it accounts for the majority of cloud storage-based malware incidents.

INFORMATION STEALERS (20-30%):

- Targeting sensitive data for financial gain or espionage, information stealers utilize cloud storage for data exfiltration after compromising systems.
- The prevalence reflects the growing value of personal and organizational data.

RANSOMWARE (10-15%):

- Ransomware attacks increasingly target cloud storage due to the concentration of valuable data contained within these environments.
- While not as frequent as cryptojacking, its impact can be devastating, making it a significant concern.

OTHER TYPES (5-10%):

- Backdoors, botnets malware, and destructive malware represent a smaller portion of cloud storage-based malware distribution.
- The emergence and prevalence can vary depending on specific trends and attacker motivations.

Exposed Buckets

Using the tools listed above, scanning a list of buckets to get files and identify misconfigured exposed buckets is possible. Below is a result of a scan for 2018-2023, according to GrayHatWarfare.

Files
2.7bn of 11.2bn

Amazon Web Services
40.8k of 312.0k

Azure Blob Storage
44.6k of 50.4k

Digital Ocean Spaces
7.0k

Google Cloud Platform
32.8k of 72.5k

Scanning using Censys together with dedicated scanning tools can provide an up-to-date list of existing buckets (see example below):

PUBLICLY AVAILABLE TOOLS

- Find misconfigured S3 buckets in a subdomain **https://github.com/suvendu-dash/misconfig-s3-bucket**
- Check S3 bucket permissions **https://github.com/clario-tech/s3-inspector**
- S3 bucket inspector looking for secrets, assets, and other sensitive staff **https://github.com/redhuntlabs/BucketLoot**
- Many other scanners, scrapers, and brute-force tools (Spartan, gobuster) include bypasses to evade alerts and pen testing frameworks
- Refer to the full list of publicly available tools: **https://github.com/mxmoz/awesome-sec-s3**

Cyber Attacks

Cloud misconfigurations have been a major source of data breaches over the past several years. In 2017, Alteryx exposed sensitive customer data when a misconfigured S3 bucket was left unsecured. In 2019, Capital One suffered a major breach when a hacker exploited an S3 bucket vulnerability to access millions of customer credit card applications. And in 2021, hackers breached security camera maker Verkada after calling AWS APIs to scan for and access insecure S3 buckets.

While the root causes vary, the common thread is that misconfigured cloud storage has repeatedly led to mass exposure of sensitive data. Unfortunately, despite increased awareness, such incidents have continued. Recently, in October 2023, India's national logistics portal left an S3 bucket exposed, compromising trade and personal data.

KNOWN S3 BUCKETS LEAKS

DATE	DESCRIPTION	NOTES
Oct 2023	India's national logistics portal exposed sensitive personal data, trade records	Exposed sensitive personal data and various state and private trade records
Aug 2022	Cloud misconfig exposes 3TB of sensitive airport data in Amazon S3 bucket: "Lives at stake"	Unsecured server exposed more than 1.5 million files, including airport worker ID photos and other PII
July 2022	McGraw Hill's S3 buckets exposed 100,000 students' grades and personal info	22TB of data and over 117 million files were exposed
Aug 2020	S3 bucket leak exposes 182GB of US and Canadian senior citizens' data	The misconfigured S3 bucket was owned by SeniorAdvisor, a consumer ratings and reviews website
July 2020	Twilio: "Someone broke into our unsecured AWS S3 silo, added 'non-malicious' code to our JavaScript SDK"	Attackers tried to update the javascript library hosted on the S3 buckets so it could be picked up by other clients
Jan 2020	"Exposed AWS buckets again implicated in multiple data leaks"	Passport scans, tax documents, background checks, job applications, expense claims, contracts, emails, and salary details relating to thousands of consultants working in the UK were exposed

DATE	DESCRIPTION	NOTES
June 2020	"7.2 million records were exposed, but not from the BHIM app"	Unsecured S3 bucket exposed BHIM user data
Oct 2018	Misconfigured database breach exposes thousands of MedCall Advisors patient files	Names, email and postal addresses, phone numbers, dates of birth, and Social Security numbers; other files had recordings of patient evaluations and conversations with doctors, along with medications, allergies, and other detailed personal health data
Jun 2019	AWS S3 server leaks data from Fortune 100 companies: Ford, Netflix, TD Bank	Attunity, an Israeli IT firm that provides data management, warehousing, and replication services for the world's biggest companies, exposed some of its customers' data after it left three Amazon S3 buckets exposed on the internet without a password
Mar 2018	Medical records and patient-doctor recordings were exposed	Information for employees of 181 business locations, as well as PII for nearly 3,000 individuals, were publicly exposed in an unsecured S3 storage bucket belonging to Medcall Healthcare Advisors
Mar 2018	Jewelry site accidentally leaks personal details (and plaintext passwords!) of 1.3 million users	Addresses, zip codes, email addresses, and IP addresses – the database claimed to contain plaintext passwords as well
Feb 2018	S3 bucket open to the world : Octoly	Real names, addresses, phone numbers, and email addresses revealed
Dec 2017	Alteryx leave S3 bucket open for anonymous user: 120 million American households exposed	Home addresses, contact information, mortgage status, and financial histories exposed
Nov 2017	111 GB of internal customer information from National Credit Federation, a Tampa, Florida-based credit repair service	SSN, drivers' licenses, credit reports, etc. exposed
Nov 2017	Uber hack exposing millions of records brought to light (months after the initial breach)	Personal information of 57 million Uber users and driver's license numbers (the initial attack itself happened months earlier)

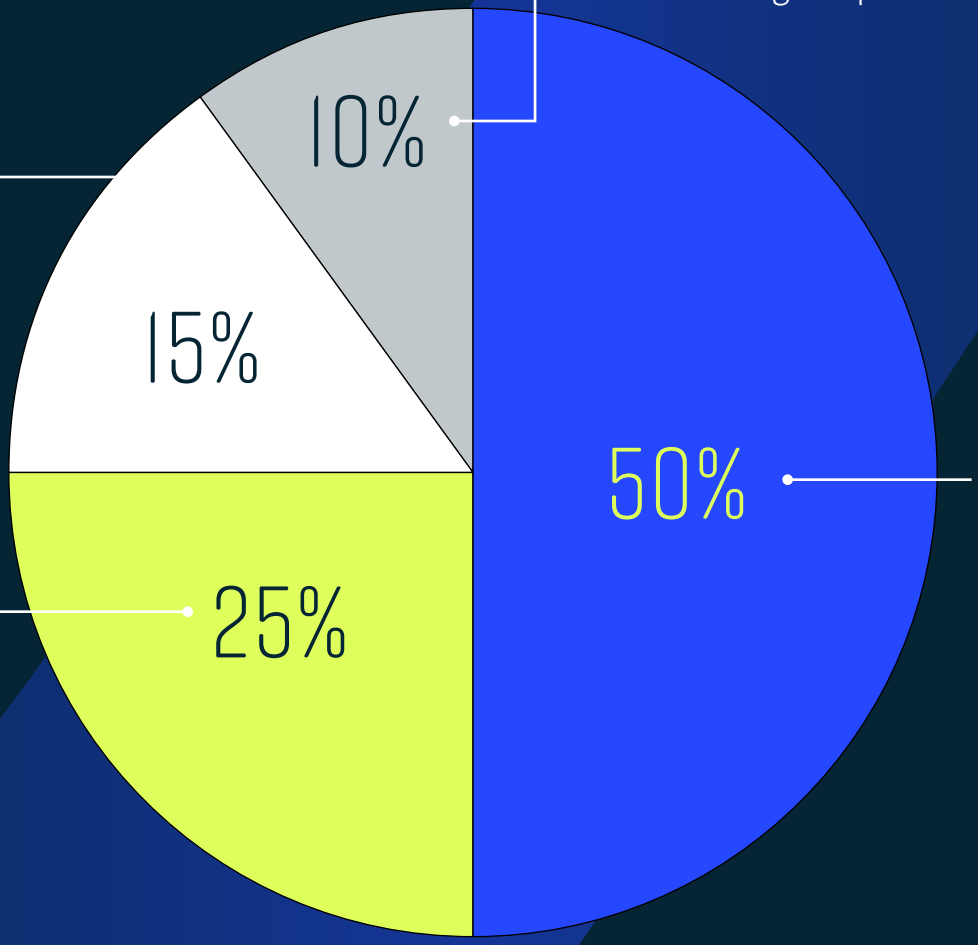
Threat Actors

There are numerous threat actor types targeting cloud storage (among other goals). Here's a breakdown of the key threat group types.

Insider Threats (10%): Motivated by personal gain, revenge, or simply carelessness, insider threats can include employees, contractors, or third-party vendors with authorized access to cloud storage. They may steal data, sabotage systems, or sell access to attackers. Sometimes, that may be caused by an "accidental data exposure" when users inadvertently share sensitive data through misconfigured permissions or insecure access methods.

Hacktivists (15%): Driven by ideological or political motivations, these actors target cloud storage to disrupt operations or raise awareness about a particular cause. They may launch denial-of-service attacks or deface websites hosted in the cloud.

Nation-State Actors (25%): Driven by espionage and geopolitical agendas, these actors target cloud storage to steal sensitive information or disrupt critical infrastructure. Their attacks are often highly sophisticated and targeted.



Cybercriminal Groups (50%): Motivated by financial gain, these groups often employ automated tools to scan for misconfigured cloud storage buckets and exploit vulnerabilities to steal data. They may then sell the stolen data on the dark web or use it for ransomware attacks.

THREAT GROUP TYPES

Threat Group in Action: TeamTNT

TeamTNT has historically targeted cloud storage environments, primarily focusing on misconfigured Kubernetes clusters, Docker APIs, Kubernetes UI tools, Redis servers, and AWS S3 buckets. They have been known to leverage these platforms for cryptojacking, deploying cryptocurrency miners in victim environments, and stealing credentials for further attacks.

KNOWN EXPLOITS TIMELINE:

- **2020-2021:** TeamTNT actively exploited vulnerabilities in cloud environments to deploy crytojacking malware and steal access credentials. They were particularly notorious for targeting open Docker APIs and misconfigured Kubernetes installations.
- **2021-2023 (AWS Focus):** In November 2021, TeamTNT announced a “retirement” via Twitter. However, researchers have observed similar malware campaigns targeting AWS S3 buckets and Docker environments throughout 2022 and 2023. These campaigns involved stealing AWS credentials, suggesting potential activity by the same threat group or copycats employing similar tactics.
- **June 2023:** SentinelOne and Permiso reported malicious actor campaigns employing tools similar to TeamTNT, focusing on credential theft from Azure and Google Cloud Platform (GCP) services alongside AWS.

Best Practices for Securing Cloud Storage

The minimum best practices to keep cloud storage safe include the following:

- **Implement least privilege access control:** Limit access to S3 buckets to authorized users and applications.
- **Enable bucket encryption:** Encrypt data at rest and in transit to protect against unauthorized access.
- **Use strong passwords and IAM roles:** Avoid hardcoded credentials and leverage identity and access management (IAM) roles for access control.
- **Monitor access logs and alerts:** Regularly review access logs and configure alerts for suspicious activity.
- **Conduct regular security assessments:** Identify and address vulnerabilities in your S3 buckets before attackers exploit them.
- **Educate users on security best practices:** Train users on phishing awareness, secure password management, and responsible cloud storage usage.
- **Scan cloud storage with an advanced AV scanner:** Implement the Deep Instinct Predictive Prevention Platform and monitor threat intelligence sources.

Conclusion

AWS S3's scalable storage is crucial for core business processes but contains unanticipated vulnerabilities. By understanding the evolving threat landscape, adopting best practices, and implementing robust security controls, organizations can significantly reduce the risk of cyberattacks and protect their sensitive data in the cloud.

References

- https://conscia.com/blog/cloud-storage-risk-assessment-our-privacy-rests-at-risk/
- https://www.einnews.com/pr_news/673477280/global-cloud-storage-market-projects-substantial-growth-set-to-reach-206-61-billion-by-2027
- https://www.fugue.co/blog/a-technical-analysis-of-the-capital-one-cloud-misconfiguration-breach
- https://github.com/nagwww/s3-leaks
- https://www.sisainfosec.com/weekly-threat-watch/new-supply-chain-attack-exploits-abandoned-aws-s3-buckets/#:~:text=New%20supply%20chain%20attack%20exploits%20abandoned%20S3%20buckets%20to%20distribute,without%20altering%20the%20modules%20themselves.
- https://checkmarx.com/blog/hijacking-s3-buckets-new-attack-technique-exploited-in-the-wild-by-supply-chain-attackers/
- https://buckets.grayhatwarfare.com/
- https://github.com/mxmoz/awesome-sec-s3