Inside Q1 2025's Most Dangerous Cloud Storage Threats

Cloudstoragesecurity.com/Contact

Table of contents

Introduction and Threat Recap

The state of global politics, recent technological advancements, and a number of other factors contribute to the constantly shifting state of the cyber threat landscape. For example in 2023, when LLMs and GenAI were arguably in their fastest state of development due to global attention, cyber threat actors managed to generate net-new malicious code using ChatGPT at a level of complexity that had "previously been reserved for nation state attackers using many resources to develop each part of the overall malware".

Cloud Storage Security's internal threat laboratory, Casmer Labs, keeps a close eye on the cyber threat landscape especially as it affects organizations who process and store data primarily in the cloud. Published in early 2025 during an analysis of The Nastiest Threats to Cloud Storage in 2024, the Casmer Labs team stated that they anticipated:

- More high-profile data breaches resulting from misconfiguration issues and ransomware attacks
- That the monetary and reputational consequences for cloud data breaches would continue to rise
- A continuation of lowering barriers to entry for malicious actions via RaaS and more sophisticated paid tools

These predictions, with a few exceptions, were proven true. In quarter 1 of 2025, the most prominent threats to organizations storing data in the cloud were:

- Misconfiguration incidents resulting in data breaches
- Ransomware attacks, both file-based and fileless
- Rapidly evolving strains of malware, particularly infostealers

Misconfiguration Incidents

In Q1 of 2025 alone, tens of millions of records were breached, exposed, or otherwise lost due to attacks leveraging cloud misconfigurations, particularly the most popular object storage service in the world, Amazon S3. Of the 10+ major misconfiguration incidents Casmer Labs became aware of, where more than 1000 records were leaked, 8 were either related or directly caused by public access to an Amazon S3 bucket (or equivalent service).

In the largest publicly disclosed data loss event of Q1 2025, Hipshipper, a US-based shipping service, exposed 14 million shipping labels by way of a publicly accessible Amazon S3 bucket. These shipping labels contained information on customer names, addresses, and contact information, making them sensitive by nature. The primary risk in exposing this information is that malicious actors could use the information within to supplement social engineering schemes, including phishing attacks. Other major data breaches that occurred in Q1 of 2025 due to a publicly accessible bucket includes the ESHYFT breach, where over 86000 healthcare records were exposed, and the Oberlin Marketing breach, where over 320000 sensitive files, most of which medicare applications, were made publicly accessible for a short period of time.

As organizations move more data, applications, and workflows into the cloud, this data tends to become more dispersed among a larger number of individual block, file, and object storage resources. Most of these major misconfigurations, in combination with a higher volume of resources that need to be maintained, are a result of human error.

Misconfiguration Incidents

IAs such, to prevent misconfiguration issues, Casmer Labs recommends that your organization takes the following steps:

- **Restrict Public Access & Secure Cloud Storage**
  - Configure strict access controls to ensure only authorized users or services can access sensitive data
  - Regularly review and update permissions to minimize exposure
- **Monitor & Audit Access Logs**
  - Continuously track access logs to detect unauthorized activity
  - Conduct retrospective log analysis to identify any suspicious access patterns
- **Encrypt Data at Rest & In Transit**
  - Enable server-side encryption to protect stored data
  - Use AWS Key Management Service (KMS) or equivalent tools to securely manage encryption keys
- **Automate Security Measures**
  - Deploy automated security checks to detect misconfigurations and vulnerabilities
  - Use cloud security tools that provide real-time alerts and automated remediation
- **Conduct Regular Security Audits**
  - Perform frequent security assessments to identify and address weak points
  - Implement penetration testing to simulate potential attacks and strengthen defenses
- **Train Employees on Cybersecurity Best Practices**
  - Educate teams on data security, phishing risks, and access control policies
  - Establish clear protocols for handling and securing sensitive information

Given that a configuration mishap on one single bucket can result in a catastrophic data breach, the regular employee training portion, at least quarterly, is one of the most important steps an organization can take to prevent data breaches before they even become an issue.

Ransomware Attacks

The popularity of both file-borne and fileless ransomware attacks also increased in Q1 of 2025. Chief in public perception were the Codefinger ransomware attacks, where an organized group of cybercriminals gained access to cloud credentials and otherwise utilized AWS native services designed to provide genuine value to their customers in a negative manner and to initiate and carry out a ransomware attack. The steps taken by the Codefinger group are outlined below:

1. AWS credentials were obtained in any one of a number of manners. Some examples are:
    a. Social engineering strategies such as phishing, which is most common
    b. Reused credentials obtained from other data breaches
    c. Ingestion and execution of infostealer-type malware
2. Once the AWS credentials are obtained, the attacker locates AWS keys with permissions to execute s3:GetObject and S3:PutObject API calls.
3. The attacker encrypts the files using AWS SSE-C.
4. The attacker sets an S3 Lifecycle policy that schedules the encrypted files for deletion within seven days.
5. The attacker leaves ransom notes in affected repositories, usually comprised of a bitcoin address, client ID, and verbiage stating that the ransom needs to be paid off in 7 days and that negotiations will cease if permissions are changed.

In order to protect against Codefinger-style attacks, Casmer Labs recommends that your organization:

- Implements a robust backup strategy, which is key to protecting against ransomware
- Adding a condition element in IAM to conditionally disable SSE-C encryption
- Enabling S3 lifecycle event notifications
- Practicing basic digital security hygiene; changing passwords frequently, enabling multi-factor authentication (MFA), etc.

While the Codefinger attacks quickly gained popularity and recognition, resulting in remediation tactics being taken quickly by organizations that operate in the cloud, Casmer Labs anticipates the further growth of fileless ransomware tactics in the months and years to come.

File-borne ransomware also saw an increase in popularity in Q1 of 2025, which will be covered below.

Malware Attacks

Casmer Labs also discovered sharp increases in the popularity of certain malware strains and families in Q1 of 2025. Chief among these is the growing popularity of infostealers, which does not come as a surprise given that cyber actors have shifted their focus towards the data plane in recent years. Generally speaking, while infostealers were not the most popular malware families discovered by Casmer Labs in Q1, they quickly ascended to the top 3 most popular malware archetypes in H2 of 2024 and Q1 of 2025.

The most popular malware archetypes logged by Casmer Labs are detailed below:

1. **Botnet Malware**: Designed against a certain operating system such as Linux to enlist and organize networked devices into a botnet, which are most commonly used to launch direct denial of service (DDoS) attacks. The most popular strains of botnet malware that were detected were Mirai and Prometei.
2. **Infostealers:** Designed to infiltrate, locate certain types of information, and exfiltrate that data without being detected. Infostealers most often serve roles in credential theft as well as sensitive information theft on a local machine. The most popular strains of infostealers that were detected were SnakeKeylogger, Formbook, and LummaStealer.
3. **RATs (Remote Access Trojans)**: Designed to give bad actors remote access to a local machine to later perform any number of malicious activities. Bad actors can monitor your local machine, initiate a ransomware attack, or otherwise steal sensitive information once a RAT has been executed. The most popular strain of RAT that was detected was RemcosRAT.

As detailed above, bad actors have slowly been shifting their focus towards away from the network and endpoint layers down to the storage and data layers. The emergence of infostealers as the more popular strains of malware is an indication of this, and should be considered when implementing proper protection for your organization's data. Aside from the best practices outlined above, Cloud Storage Security and Casmer Labs recommends that your organization:

- Scans Data in Storage Regularly for Malware: Leverage in-tenant malware protection to ensure that malicious files are detected before they are distributed downstream and accessed
- Automates Threat Detection: Implement cloud-native security tools that scan uploaded files in real time to prevent malware from propagating
- Enforces Access Control and Encryption: Enforce strict access policies and encrypt stored data to reduce exposure
- Implements Continuous Monitoring Practices and Habits: Regularly audit cloud storage configurations and access logs to detect anomalies

Conclusion and Forward Outlook

Casmer Labs has discovered and monitors a number of distinct threats to organizations that store and process their data in the cloud. Chief among these threats is that of misconfigurations, which has arguably caused the greatest number of data breaches in terms of records alone in Q1 of 2025.

In the balance of 2025, Casmer Labs anticipates that bad actors' focus will continue to shift towards the data layer, with the following consequences:

- More high-profile data breaches resulting from misconfiguration issues and ransomware attacks
- That the monetary and reputational consequences for cloud data breaches will continue to rise
- A continuation of lowering barriers to entry for malicious actors via RaaS and more sophisticated paid tools

About Cloud Storage Security

,

Cloud Storage Security (CSS) offers customers the ability to deploy multi-cloud, multi-account, and multi-resource malware scanning to protect the entirety of their storage suite under one console. Customers choose CSS' solution because it:

- **Offers flexible scanning models** – Scan existing data on a scheduled basis, as data is written to storage repositories, or even before it is written
- **Offers multiple malware scanning engines** – Using multiple enterprise-grade engines reduce false positives and false negative rates
- **Is simple to deploy, configure, and live with** – Initial deployment can be performed in under 15 minutes. In-console quarantine, the ability to set up scanning for all storage resources in a single click, and minimal maintenance can all be performed from the console

Cloud Storage Security (CSS) also provides customers with flat-rate pricing based on cloud spend or no. of employees, that allows customers to:

- Apply malware protection for their *entire* environment, including Amazon S3, Amazon EFS, Amazon EBS, Amazon FSx, Microsoft Azure Blob Storage, and Google Cloud Buckets
- Perform periodic rescanning to meet compliance requirements and detect dormant malware

If your organization is interested in learning more about securing its storage resources, get in contact with an SME at cloudstoragesecurity.com/contact or watch an in-depth demo at cloudstoragesecurity.com.

Organizations can also try out the solution for free for 30 days in AWS Marketplace.

About Cloud Storage Security

Cloud Storage Security protects data in the cloud and on premises so that businesses can move forward freely and fearlessly. Our robust solutions are born from a singular focus on, and dedication to, securing the world's data, everywhere. Cloud Storage Security builds modular solutions that identify, mitigate, and eliminate today's risks and the ones to come. We solve security and compliance challenges by identifying and eliminating threats, while reducing risk and human error.

021225