
CLOUD
STORAGE SECURITY
Casmer Labs Presents:
Quarter 2 Threat Report
Cloudstoragesecurity.com/Contact

Table of contents

\-

Introduction and Threat Recap

The cyber threat landscape is in constant flux, shaped by global politics, technological progress, and other constantly evolving factors. In 2023, we witnessed one of the first instances of ChatGPT being used to create new malicious code. In 2024, we witnessed the rise of infostealers and a number of high-profile attacks on federal government and Fortune 500 organizations. In 2025, particularly in Q2, a number of other alarming trends have come to fruition.

Casmer Labs, Cloud Storage Security's internal threat laboratory, diligently monitors the cyber threat landscape, with a particular focus on its impact on organizations that primarily process and store data in the cloud. During our threat report covering Q1 of 2025, the Casmer Labs team projected:

- An increase in high-profile data breaches stemming from misconfiguration issues and ransomware attacks.
- A continued escalation of both the financial and reputational repercussions associated with cloud data breaches.
- A persistent lowering of barriers to entry for malicious actors, driven by the prevalence of Ransomware-as-a-Service (RaaS) and the emergence of more advanced paid tools.

In many ways, the cyber threat landscape has evolved since Q1. In Q2, the most prominent threats to organizations storing data in the cloud were:

- Lack of monitoring resulting in both internal and external threats
- Misconfiguration issues causing data breaches
- Rapidly evolving strains of malware as a part of ransomware-as-a-service (RaaS) vendors

Lack of Monitoring

In Q2 of 2025, we witnessed a number of high-profile data breaches and cybersecurity incidents resulting from the lack of activity monitoring functionality on behalf of the victim. Chief of these incidents was the Coinbase attack, where overseas support employees exfiltrated sensitive information on behalf of cyber actors. On the day of its public announcement on May 15, 2025, Coinbase (COIN) closed down 7% following concerns about internal policies and an open SEC investigation. While many organizations hire large security teams to prevent these issues, the simple truth of the matter is that without the combination of employee education and activity monitoring, **no amount of controls will ever be able to stop a determined actor attempting to carry out a similar attack.** While it is still unclear whether or not the overseas employees were granted excessive permissions to perform their jobs (such as being able to access or download sensitive customer information), an effective activity monitoring solution would have been able to detect this anomaly and prevent more data from being exfiltrated.

Another high-profile attack that took place in Q2 of 2025 was the Ingram Micro incident, where attackers reportedly compromised Ingram Micro's systems via their VPN, causing a total downtime of ~5 days. At the time of the publication of this whitepaper, it is likely that the compromise of the VPN systems resulted in the encryption and ransom of all systems, including Ingram Micros' cloud storage. Similar to the Coinbase incident described above, a competent, automated activity monitoring solution would have prevented the encryption and loss of Ingram Micro's data.

Other smaller incidents, including an attack on Columbia University, also occurred in Q2 of 2025.

To prevent similar attacks from affecting your organization, Casmer Labs recommends that the following best practices are followed:

- Implement a robust backup strategy, which is key to protecting against ransomware
- Adding a condition element in IAM to conditionally disable SSE-C encryption
- Enable S3 lifecycle event notifications
- Practicing basic digital security hygiene; changing passwords frequently, enabling multi-factor authentication (MFA), etc.
- Implement a signature-based and anomaly detection activity monitoring solution that proactively parses logs to identify early indicators of breaches and ransomware attacks

DataDefender by Cloud Storage Security automates the detection and mitigation of threats, internal or external, preventing data exfiltration, ransomware, and other threats at the source. Sign up for the DataDefender beta here.

Misconfiguration Issues

In Q2 of 2025, Casmer Labs identified over 15 misconfiguration incidents that resulted in a major data breach (1000+ records accessed/lost). Of these incidents, 11 were related to popular object storage services such as Amazon S3, Microsoft Azure Blob, and Google Cloud Storage.

In the largest publicly disclosed data loss event of Q2 2025, employee monitoring software WorkComposer inadvertently exposed 21 million screenshots taken by the service via a publicly accessible Amazon S3 bucket. As of April 28, 2025, the leaked screenshots were confirmed to include login credentials, API keys, internal emails, and calendar appointments. Aside from the obvious risks associated with leaked credentials, similar to the HipShipper incident in Q1 of 2025, the information could be used by cyber actors to supplement phishing and social engineering schemes.

With a growing number of organizations migrating their data, applications, and workflows to the cloud, there's a corresponding increase in data dispersion across various block, file, and object storage resources. This rise in misconfigurations, often coupled with an expanded volume of resources requiring maintenance, is primarily attributable to human error. To proactively address and mitigate these misconfiguration issues, Casmer Labs advises organizations to implement the following measures:

- **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'
- **Implement Automated Tools to Manage Configuration**
  - Ensure these tools can identify misconfigurations at scale and automatically remediate the issues, if necessary

DataDefender by Cloud Storage Security monitors 90+ configuration options over 10 cloud services, including Amazon S3, Amazon EBS, Amazon EFS, and Amazon FSx. When an issue, such as a publicly accessible Amazon S3 bucket or Amazon EBS snapshot is detected, the problem can be automatically or manually remediated before a data breach occurs. Sign up for the DataDefender beta here.

Malware and Ransomware-as-a-Service

In Q1 of 2025, Casmer Labs predicted the continuing rise of malware, particularly infostealers, and the number of victims claimed by ransomware-as-a-service (RaaS) vendors. In Q2 of 2025, both of these proved to be true.

SafePay, the attacker suspected of compromising Ingram Micro, has been suspected to have victimized over 200 organizations since they emerged in November of 2024. While it should be noted that large ransomware gangs such as LockBit, Black Cat, RansomHub, Everest, and BlackLock have all suffered abrupt cessations or failures in the past 6 months, other gangs are quickly taking their places. Take for example the Qilin ransomware gang, who recently gained notoriety for providing legal counsel to their customers to extract more money from their victims.

When covering file-based malware, infostealers were the top family of malware detected by Casmer Labs in Q2 of 2025, jumping up 2 spots from #3 in Q1.

Bad actors are increasingly targeting the storage and data layers, shifting their focus away from network and endpoint layers. The rise of infostealers as a prevalent malware strain underscores this trend and should be a key consideration in your organization's data protection strategy. In addition to the best practices previously mentioned, Cloud Storage Security and Casmer Labs recommend 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 the lack of activity monitoring, and misconfigurations, which have claimed hundreds of victims alone in Q2 of 2025. As organizations continue to navigate the fast-moving world of cyber threats, one thing remains clear; given the sheer scale of the IT infrastructure that most organizations maintain, only so much can be done to prevent breaches without the usage of competent, automated, focused tools.

About Cloud Storage Security
Cloud Storage Security (CSS) offers customers the ability to protect the storage layer in their cloud environments. DataDefender by Cloud Storage Security offers customers complete protection over the entirety of their cloud storage environment. Make sure your organization:

- Knows where its sensitive data resides
- Configures their storage resources in a secure manner
- Prevents the ingestion and distribution of malware, including ransomware
- Identifies and stops internal and external attacks against storage, and the data within

The DataDefender beta program is open for applications now. Sign up at cloudstoragesecurity.com/datadefender to request access to the solution.

Cloud Storage Security's cloud antivirus solution is also available in AWS Marketplace with a 30-day free trial.

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