Research Threat intelligence Microsoft Defender for Cloud Cloud threats
**7 min read**

# Cloud storage security: What's new in the threat matrix

By Microsoft Threat Intelligence

**September 7, 2023**

Cloud security

Microsoft Defender

Today, we announce the release of a second version of the threat matrix for storage services, a structured tool that assists in identifying and analyzing potential security threats on data stored in cloud storage services. The matrix, first released in April 2021 as detailed in the blog post Threat matrix for storage services, lays out a rich set of attack techniques mapped to a well-known set of tactics described by MITRE's ATT&CK® framework and comprehensive knowledge base, allowing defenders to more efficiently and effectively adapt and respond to new techniques.

Cybercriminals target cloud storage accounts and services for numerous purposes, such as accessing and exfiltrating sensitive data, gaining network footholds for lateral movement, enabling access to additional resources, and deploying malware or engaging in extortion schemes. To combat such threats, the updated threat matrix provides better coverage of the attack surface by detailing several new initial access techniques. The matrix further provides visibility into the threat landscape by detailing several novel attacks unique to cloud environments, including some not yet observed in real attacks. The new version of the matrix is available at: https://aka.ms/StorageServicesThreatMatrix

Figure 1. Threat matrix for storage services

Of the new techniques detailed in this blog, several noteworthy examples include:

- **Object replication** – Allows attackers to maliciously misuse the object replication feature in both directions by either using outbound replication to exfiltrate data from a target storage account or using inbound replication to deliver malware to the target account.
- **Operations across geo replicas** – Helps attackers evade defenses by distributing operations across geographical copies of storage accounts. Security solutions may only have visibility into parts of the attack and may not detect enough activity in a single region to trigger an alert.
- **Static website** – Allows attackers to exfiltrate data using the "static website" feature, a feature provided by major storage cloud providers that can often be overlooked by less experienced users.

In this blog post, we'll introduce new attack techniques that have emerged since our last analysis and cover the various stages of a potential attack on cloud storage accounts.

## New techniques in the matrix

## 1. Reconnaissance

Reconnaissance consists of techniques that involve attackers actively or passively gathering information that can be used to support targeting.

**DNS/Passive DNS** – Attackers may search for DNS data for valid storage account names that can become potential targets. Threat actors can query nameservers using brute-force techniques to enumerate existing storage accounts in the wild, or search through centralized repositories of logged DNS query responses (known as passive DNS).

**Victim-owned websites** – Attackers may look for storage accounts of a victim enterprise by searching its websites. Victim-owned website pages may be stored on a storage account or contain links to retrieve data stored in a storage account. The links contain the URL of the storage and provide an entry point into the account.

## 2. Initial access

Initial access consists of techniques that use various entry vectors to gain their initial foothold on a storage account. Once achieved, initial access may allow for continued access, data exfiltration, or lateral movement through a malicious payload that is distributed to other resources.

**SFTP credentials** – Attackers may obtain and abuse credentials of an SFTP (Secure File Transfer Protocol) account as a means of gaining initial access. SFTP is a prevalent file transfer protocol between a client and a remote service. Once the user connects to the cloud storage service, the user can upload and download blobs and perform other operations that are supported by the protocol. SFTP connections require SFTP accounts, which are managed locally in the storage service instance, including credentials in the form of passwords or key-pairs.

**NFS access** – Attackers may perform initial access to a storage account using the NFS protocol where enabled. While access is restricted to a list of allowed virtual networks that are configured on the storage account firewall, connection via NFS protocol does not require authentication and can be performed by any source on the specified networks.

**SMB access** – Attackers may perform initial access to a storage account file shares using the Server Message Block (SMB) protocol.

**Object replication** – Attackers may set a replication policy between source and destination containers that asynchronously copies objects from source to destination. This feature can be maliciously misused in both directions. Outbound replication can serve as an exfiltration channel of customer data from the victim's container to the adversary's container. Inbound replication can be used to deliver malware from an adversary's container to a victim's container. After the policy is set, the attacker can operate on their container without accessing the victim container.

## 3. Persistence

Persistence consists of techniques that attackers use to keep access to the storage account due to changed credentials and other interruptions that could cut off their access. Techniques used for persistence include any access, action, or configuration changes that let them maintain their foothold on systems.

**Create SAS Token** – Attackers may create a high-privileged SAS token with long expiry to preserve valid credentials for a long period. The tokens are not monitored by storage accounts, thus they cannot be revoked (except Service SAS) and it's not easy to determine whether there are valid tokens in the wild until they are used.

**Container access level property** – Attackers may adjust the container access level property at the granularity of a blob or container to permit anonymous read access to data in the storage account. This configuration secures a channel to exfiltrate data even if the initial access technique is no longer valid.

**SFTP account** – Attackers may create an SFTP account to maintain access to a target storage account. The SFTP account is local on the storage instance and is not subject to Azure RBAC permissions. The account is also unaffected in case of storage account access keys rotation.

**Trusted Azure services** – Attackers may configure the storage account firewall to allow access by trusted Azure services. Azure Storage provides a predefined list of trusted services. Any resource from that list that belongs to the same subscription as the storage account is allowed by the firewall even if there is no firewall rule that explicitly permits the source address of the resource.

**Trusted access based on a managed identity** – Attackers may configure the storage account firewall to allow access by specific resource instances based on their system-assigned managed identity, regardless of their source address. The resource type can be chosen from a predefined list provided by Azure Storage, and the resource instance must be in the same tenant as the storage account. The RBAC permissions of the resource instance determine the types of operations that a resource instance can perform on storage account data.

**Private endpoint** – Attackers may set private endpoints for a storage account to establish a separate communication channel from a target virtual network. The new endpoint is assigned with a private IP address within the virtual network's address range. All the requests sent to the private endpoint bypass the storage account firewall by design.

## 4. Defense evasion

The defense evasion tactic consists of techniques that are used by attackers to avoid detection and hide their malicious activity.

**Disable audit logs** – Attackers may disable storage account audit logs to prevent event tracking and avoid detection. Audit logs provide a detailed record of operations performed on a target storage account and may be used to detect malicious activities. Thus, disabling these logs can leave a resource vulnerable to attacks without being detected.

**Disable cloud workload protection** – Attackers may disable the cloud workload protection service which raises security alerts upon detection of malicious activities in cloud storage services.

**Private endpoint** – Attackers may set private endpoints for a storage account to establish a separate communication channel from a target virtual network. The new endpoint is assigned with a private IP address within the virtual network's address range. All the requests sent to the private endpoint bypass the storage account firewall by design.

**Operations across geo replicas** – Attackers may split their requests across geo replicas to reduce the footprint in each region and avoid being detected by various rules and heuristics.

## 5. Credential access

Credential access consists of techniques for stealing credentials like account names and passwords. Using legitimate credentials can give adversaries access to other resources, make them harder to detect, and provide the opportunity to help achieve their goals.

**Unsecured communication channel** – Attackers may sniff network traffic and capture credentials sent over an insecure protocol. When a storage account is configured to support unencrypted protocol such as HTTP, credentials are passed over the wire unprotected and are susceptible to leakage. The attacker can use the compromised credentials to gain initial access to the storage account.

## 6. Discovery

Discovery consists of techniques attackers may use to gain knowledge about the service. These techniques help attackers observe the environment and orient themselves before deciding how to act.

**Account configuration discovery** – Attackers may leverage control plane access permission to retrieve the storage account configuration. The configuration contains various technical details that may assist the attacker in implementing a variety of tactics. For example, firewall configuration provides network access information. Other parameters may reveal whether access operations are logged. The configuration may also contain the backup policy that may assist the attacker in performing data destruction.

## 7. Exfiltration

Exfiltration consists of techniques that attackers may use to extract data from storage accounts. These may include transferring data to another cloud storage outside of the victim account and may also include putting size limits on the transmission.

**Static website** – Attackers may use the "static website" feature to exfiltrate collected data outside of the storage account. Static website is a cloud storage provider hosting capability that enables serving static web content directly from the storage account. The website can be reached via an alternative web endpoint which might be overlooked when restricting access to the storage account.

**Object replication** – Attackers may set a replication policy between source and destination containers that asynchronously copies objects from source to destination. Outbound replication can serve as an exfiltration channel of customer data from a

victim's container to an adversary's container.

## Conclusion

As the amount of data stored in the cloud continues to grow, so does the need for robust security measures to protect it. Microsoft Defender for Cloud can help detect and mitigate threats on your storage accounts. Defender for Storage is powered by Microsoft Threat Intelligence and behavior modeling to detect anomalous activities such as sensitive data exfiltration, suspicious access, and malware uploads. With agentless at-scale enablement, security teams are empowered to remediate threats with contextual security alerts, remediation recommendations, and configurable automations. Learn more about Microsoft Defender for Cloud support for storage security.

**Evgeny Bogokovsky**

*Microsoft Threat Intelligence*

## References

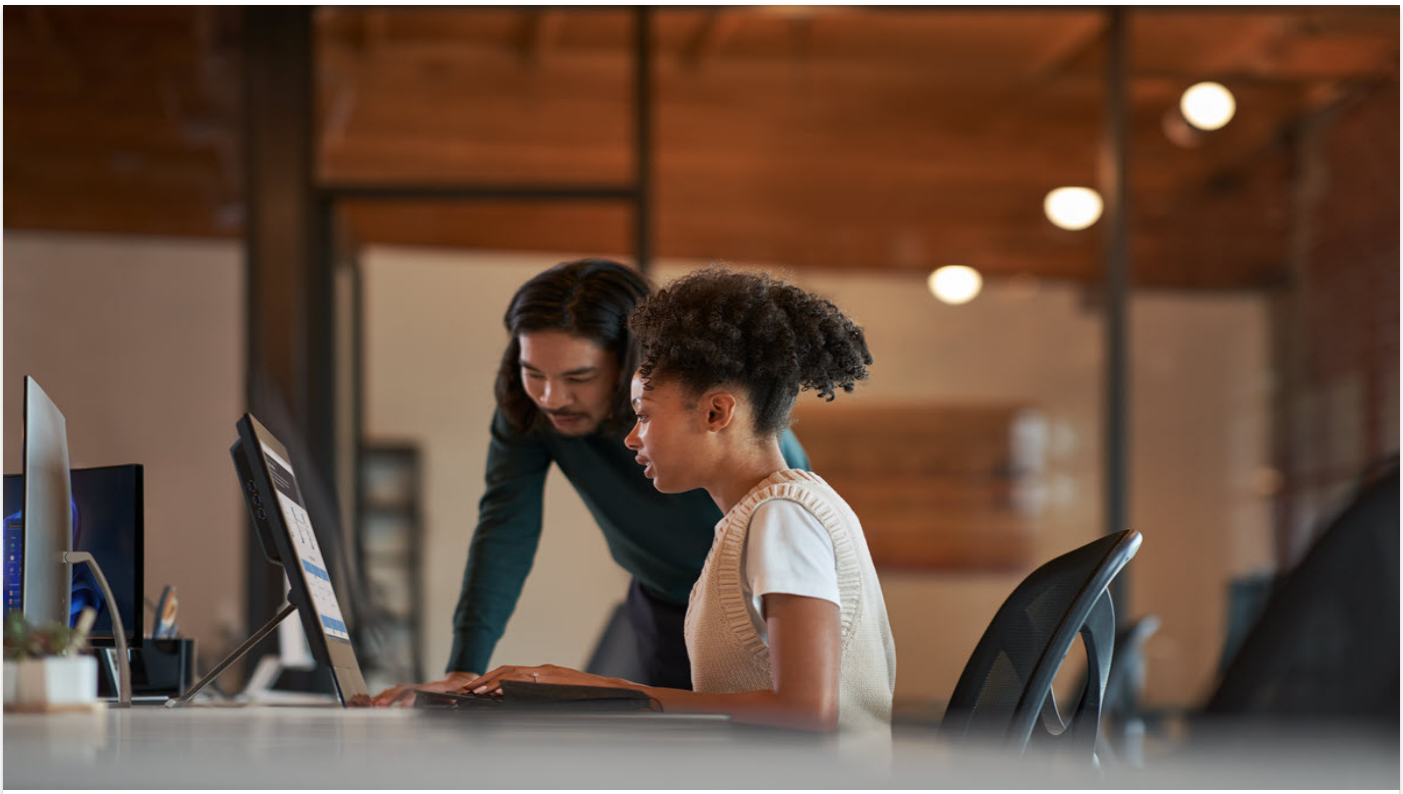
- https://attack.mitre.org/

## Further reading

For the latest security research from the Microsoft Threat Intelligence community, check out the Microsoft Threat Intelligence Blog: https://aka.ms/threatintelblog.

To get notified about new publications and to join discussions on social media, follow us on Twitter at https://twitter.com/MsftSecIntel.

## Related Posts



**Research**
**Threat intelligence**

**Apr 6**
**10 min read**

## DevOps threat matrix

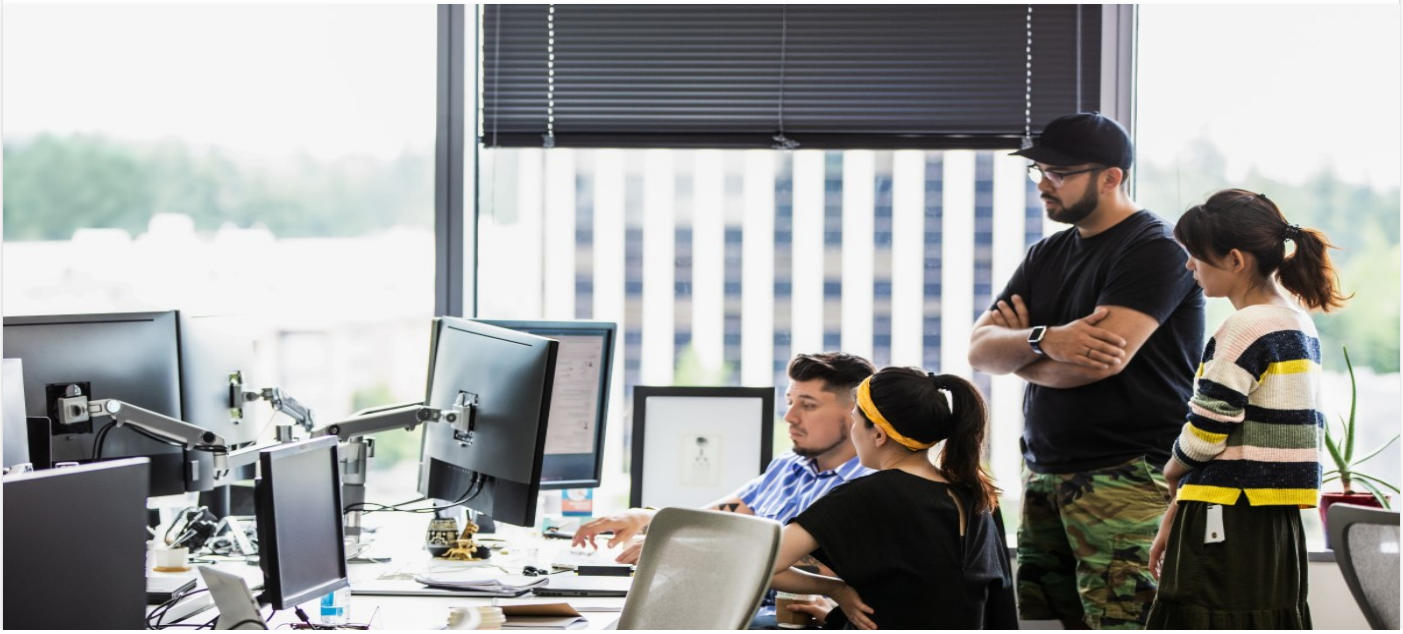
In this blog, we discuss threats we face in our DevOps environment, introducing our new threat matrix for DevOps. Using this matrix, we show the different techniques an adversary might use to attack an organization from the initial access phase and forward.

Research
Threat intelligence
Microsoft Defender
Threat actors

**Dec 7**
**4 min read**

## Mitigate threats with the new threat matrix for Kubernetes

The updated threat matrix for Kubernetes comes in a new format that simplifies usage of the knowledge base and with new content to help mitigate threats.



News
Threat trends

**Jul 21**
**5 min read**

### The evolution of a matrix: How ATT&CK for Containers was built

As containers become a major part of many organizations' IT workloads, it becomes crucial to consider the unique security threats that target such environments when building security solutions. The first step in this process is understanding the relevant attack landscape.

News
Security management
Microsoft Defender

**Apr 8**
**10 min read**

### Threat matrix for storage services

Storage services are one of the most popular services in the cloud. In this blog, we outline potential risks that you should be aware of when deploying, configuring, or monitoring your storage environment.

## Get started with Microsoft Security

Microsoft is a leader in cybersecurity, and we embrace our responsibility to make the world a safer place.

**Learn more**

Connect with us on social

### What's new

Surface Laptop Studio 2

Surface Laptop Go 3

Surface Pro 9

Surface Laptop 5

Microsoft Copilot

Copilot in Windows

Explore Microsoft products

Windows 11 apps

### Microsoft Store

Account profile

Download Center

Microsoft Store support

Returns

Order tracking

Certified Refurbished

Microsoft Store Promise

Flexible Payments

### Education

Microsoft in education

Devices for education

Microsoft Teams for Education

Microsoft 365 Education

How to buy for your school

Educator training and development

Deals for students and parents

Azure for students

### Business

Microsoft Cloud

Microsoft Security

Dynamics 365

Microsoft 365

Microsoft Power Platform

Microsoft Teams

Copilot for Microsoft 365

Small Business

## Developer & IT

Azure

Developer Center

Documentation

Microsoft Learn

Microsoft Tech Community

Azure Marketplace

AppSource

Visual Studio

## Company

Careers

About Microsoft

Company news

Privacy at Microsoft

Investors

Diversity and inclusion

Accessibility

Sustainability

English (United States)

Your Privacy Choices

Consumer Health Privacy