


A complex network diagram with numerous nodes and connecting lines, rendered in shades of blue and purple. The nodes are represented by small squares and circles, some containing numerical values like 67.44, 27.15, 48.15, 15.79, 59.33, 26.37, 56.10, 31.75, and 79.93. The lines represent connections between these nodes, creating a dense web of relationships.

Martin Haller

《 RansomCloud:
Ransomware
Operations in
Microsoft 365 》

PATRON 《IT》 OCHRANA
A SPRÁVA SÍTÍ

- Search Mail and People
- ← Folders
- ^ Favorites
 - Inbox
 - Sent Items
 - Drafts
 - ^ Kevin Mitnick
 - Inbox**
 - Drafts
 - Sent Items
 - Deleted Items 1
 - Archive
 - Conversation History
 - Junk Email
 - Notes
 - ^ Groups
 -  Groups give teams a shared space for email, documents, and scheduling events.
 - Discover
 - + Create


New | Mark all as read

Inbox

Filter | Agenda

Next: No events for the next two days.

Kevin Mitnick	Art inSight, February 2018	1:16 PM
Kevin Mitnick	Watch the "End Game" Official Music Video + New	1:16 PM
Kevin Mitnick	Tech fails at CES	1:16 PM
Kevin Mitnick	(1) invite: the DENIM you'll want to wear every day	1:16 PM
Kevin Mitnick	Talk about FriYAY! Take up to 50% OFF storewide	1:16 PM
Kevin Mitnick	Our best-selling jeans are 50% off!	1:16 PM
Kevin Mitnick	Jan 12-26: Film preservation fest, Andrey Zvyagints	1:16 PM
Kevin Mitnick	PRICE CUT! Take an EXTRA 40% off Clearance	1:16 PM



Select an item to read

[Click here to always select the first item in the list](#)

Disclaimer

This lecture presents the topic from an attacker's perspective, solely to provide a better understanding of the mindset, motivations, and techniques that hackers use in practice.

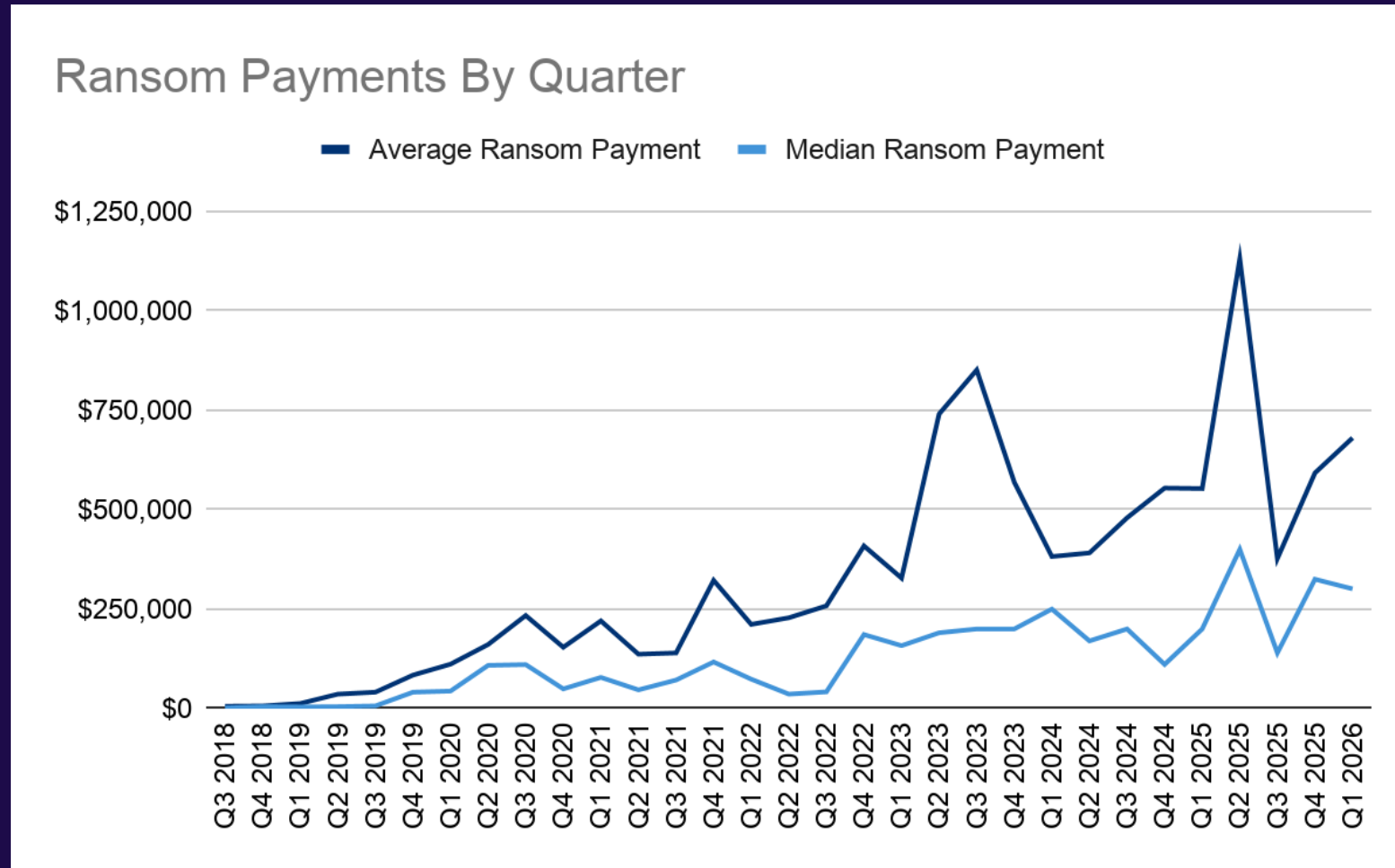
All information is intended exclusively for defensive, educational, and legal purposes. I am, and always will be, on the side of defenders, security professionals, and applicable law.

Nothing discussed here may be tested on systems, data, or infrastructure that you do not own, or for which you do not have explicit authorization. Any unauthorized testing or interference with third-party systems is illegal.

The purpose of this lecture is to improve security, not to provide instructions for causing harm.

Is Cloud Ransomware Feasible?

Is Cloud Ransomware Worth the Effort?



Source: <https://coveware.com/2026/04/patch-management-goes-from-hard-to-ludicrous-in-the-agentic-ai-era/>

How Could Cloud Ransomware Be Carried Out?

Where is the Data Stored?

Exchange Online



OneDrive



SharePoint Online



(Teams)



Azure

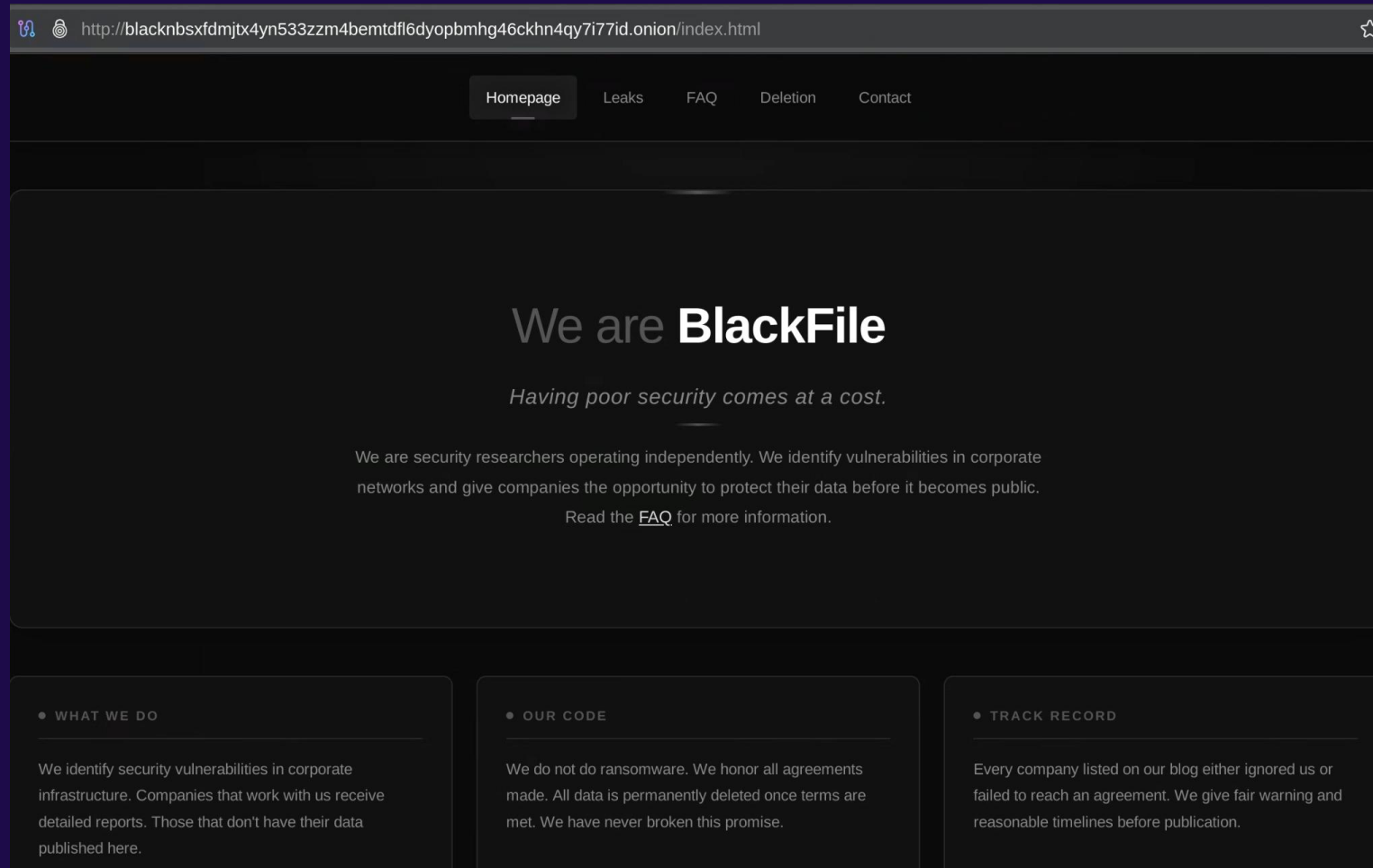


Step 0) Data Exfiltration

Octo Tempest employs a unique technique using the data movement platform Azure Data Factory and automated pipelines to extract data to external actor hosted Secure File Transfer Protocol (SFTP) servers, aiming to blend in with typical big data operations. Additionally, the threat actor commonly registers legitimate Microsoft 365 backup solutions such as Veeam, AFI Backup, and CommVault to export the contents of SharePoint document libraries and expedite data exfiltration.

Source: <https://www.microsoft.com/en-us/security/blog/2023/10/25/octo-tempest-crosses-boundaries-to-facilitate-extortion-encryption-and-destruction/>

Step 0) Data Exfiltration & Extortion



Source: <https://cloud.google.com/blog/topics/threat-intelligence/blackfile-vishing-extortion-operation/>

Step 1) Exchange Online

Exchange Online – À la Kevin Mitnick

The image displays two side-by-side screenshots of an email inbox interface, likely from Microsoft Exchange Online. Both screenshots show a list of emails from 'Kevin Mitnick'. The left screenshot shows a list of promotional emails from February 2018, including 'Art inSight, February 2018', 'Watch the "End Game" Official Music Video + New Order reputation now!', 'Tech fails at CES', '(1) invite: the DENIM you'll want to wear every day', 'Talk about FriYAY! Take up to 50% OFF storewide', 'Our best-selling jeans are 50% off!', 'Jan 12-26: Film preservation fest, Andrey Zvyagintsov', and 'PRICE CUT! Take an EXTRA 40% off Clearance'. The right screenshot shows a list of promotional emails from January 2018, including '[INFECTED] Talk about FriYAY! Take up to 50% OFF storewide', '[INFECTED] Our best-selling jeans are 50% off!', '[INFECTED] Jan 12-26: Film preservation fest, Andre', '[INFECTED] PRICE CUT! Take an EXTRA 40% off Clearance', '[INFECTED] It's happening! 40% off + extra 20% off', '[INFECTED] Extra 20% off. Translation: extra JOY', '[INFECTED] Journey', and '[INFECTED] (1 new message) You've been granted a'. A red arrow points from the first email in the right screenshot to the first email in the left screenshot, indicating a message move or copy action.



Recycle Bin



Microsoft Edge



Google Chrome

Finance headline
US Crude Oil Inv...



Search



ENG

2:02 PM
11/13/2025

Step 2) OneDrive

OneDrive – Challenges

- » **Encryption** = download the data, encrypt it, upload it
- » Version history
- » Soft delete — different levels of recycle bins
- » **Solution** = delete the entire OneDrive (<https://learn.microsoft.com/en-us/sharepoint/restore-deleted-onedrive>)

Permanently delete a OneDrive

After you recover the data you need from the OneDrive, we recommend that you permanently delete the OneDrive by running the following command:

PowerShell

Copy

```
Remove-SPOSite -Identity <URL>  
Remove-SPODeletedSite -Identity <URL>
```

⊗ Caution

When you permanently delete a OneDrive, you won't be able to restore it.

Step 3) SharePoint

SharePoint – Challenges

- » Same situation as OneDrive
- » Microsoft has backups going back up to 14 days (<https://learn.microsoft.com/en-us/compliance/assurance/assurance-sharepoint-online-data-deletion>)

SharePoint retains backups of all content for 14 additional days beyond actual deletion to facilitate a full site collection restore for customers. Customers can reach out to Microsoft support to initiate a full site collection or sub-site [point in time restore](#) if files are hard deleted, corrupted, or infected with malware and are unrecoverable using the methods described earlier. After this 14 day period, Microsoft no longer retains the data and it isn't recoverable.

- » **Solution** = <https://www.proofpoint.com/us/blog/cloud-security/proofpoint-discovers-potentially-dangerous-microsoft-office-365-functionality>

Step 4) Customer backups



Recycle Bin



Microsoft Edge



Google Chrome

Finance headline
US Crude Oil Inv...



Search



ENG

2:02 PM
11/13/2025

Step 5) Cache on Workstations

Cache on Workstations

Stryker attack wiped tens of thousands of devices, no malware needed

By [Ionut Ilascu](#)

March 16, 2026 03:17 PM 3



Last week's cyberattack on medical technology giant Stryker was limited to its internal Microsoft environment and remotely wiped tens of thousands of employee devices

Source: <https://www.bleepingcomputer.com/news/security/stryker-attack-wiped-tens-of-thousands-of-devices-no-malware-needed/>



Recycle Bin



Microsoft Edge



Google Chrome

Finance headline
US Crude Oil Inv...



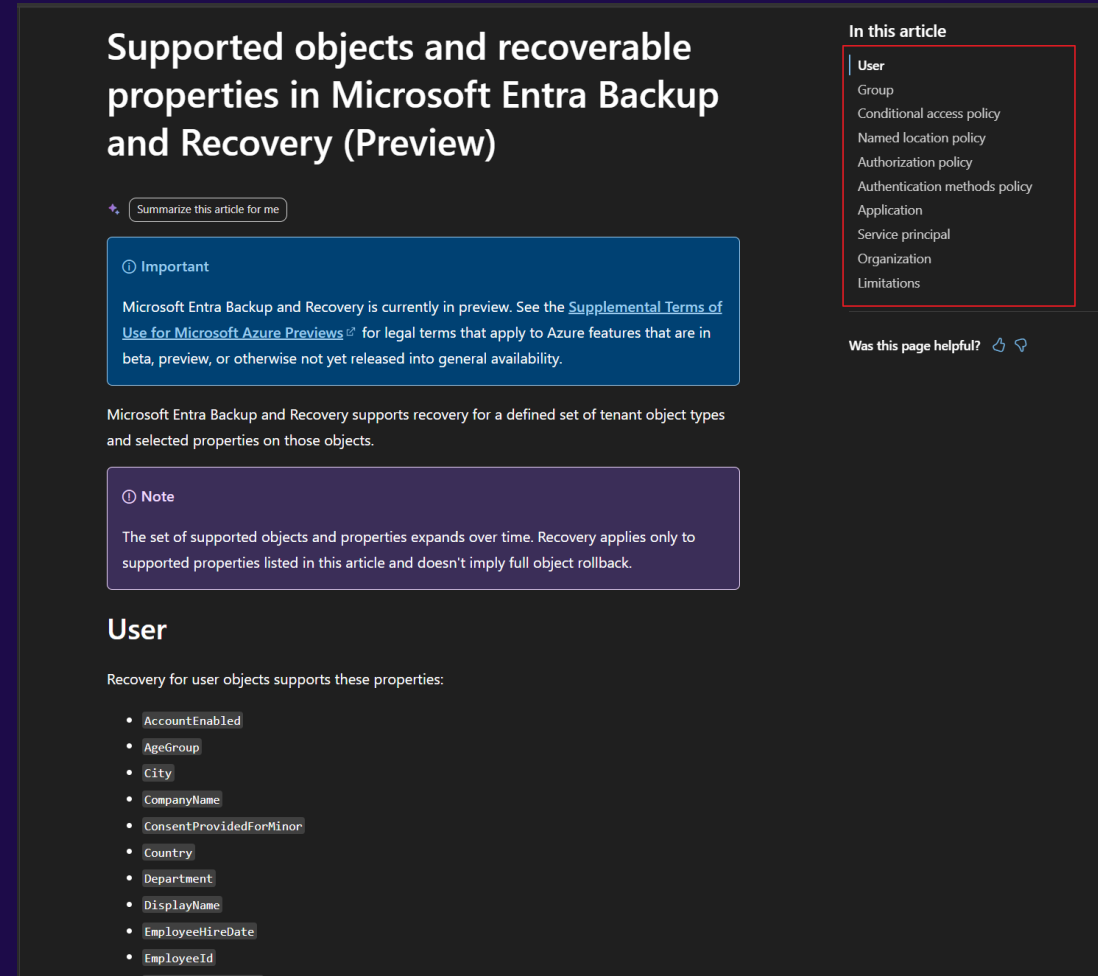
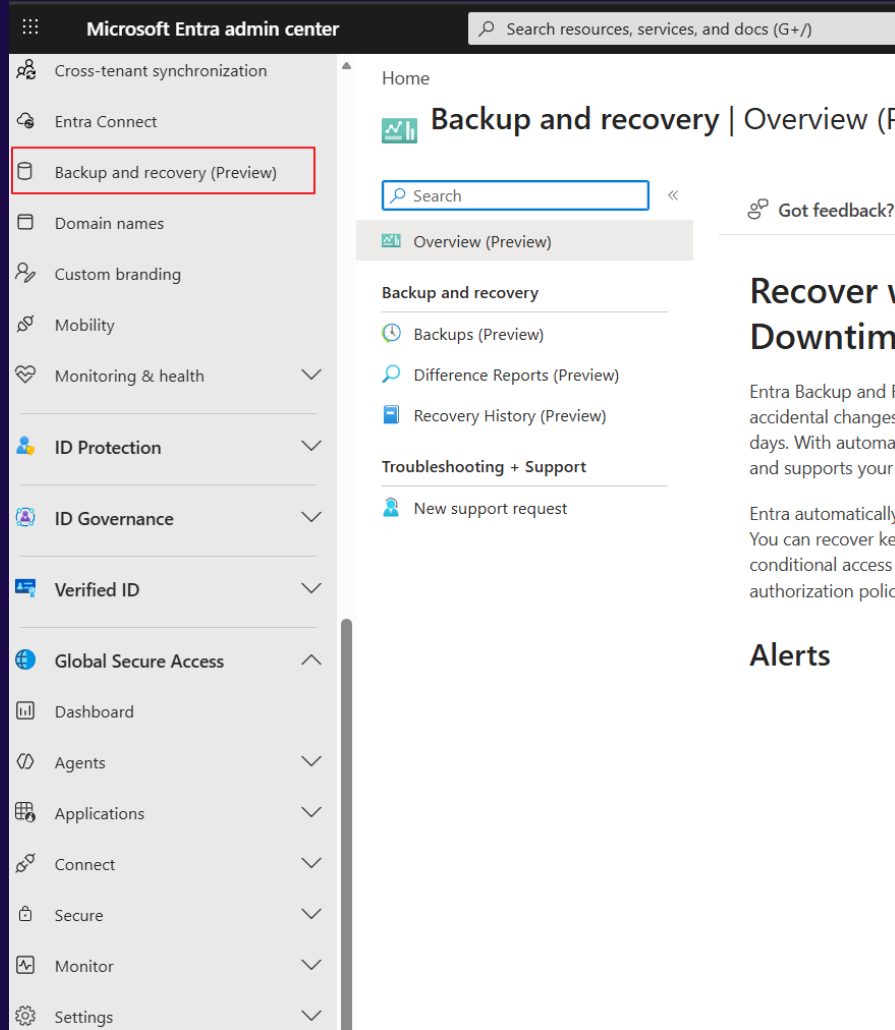
Search



ENG

2:02 PM
11/13/2025

Cache on Workstations

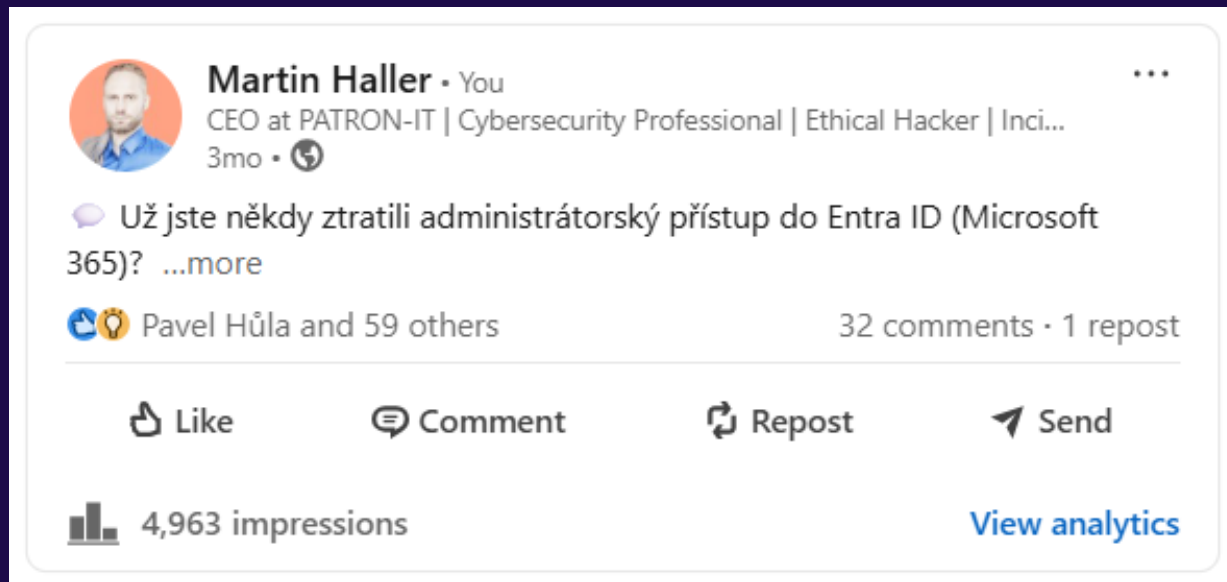


Source: <https://learn.microsoft.com/en-us/entra/backup/scope-supported-objects-limitations>

Step 6) Blocking Administrators

Blocking Administrators

- » They need to buy time and have a quiet environment to work.
- » A new aspect compared to on-prem ransomware.
- » Without support, they won't regain access.



The screenshot shows a LinkedIn post from Martin Haller, CEO at PATRON-IT. The post is in Czech and discusses losing administrative access to Entra ID (Microsoft 365). It has 32 comments and 1 repost, with 4,963 impressions.

Martin Haller • You
CEO at PATRON-IT | Cybersecurity Professional | Ethical Hacker | Inci...
3mo • 🌐

🗨️ Už jste někdy ztratili administrátorský přístup do Entra ID (Microsoft 365)? ...more

👍👤 Pavel Hůla and 59 others 32 comments · 1 repost

👍 Like 💬 Comment 🔄 Repost ↗️ Send

📊 4,963 impressions [View analytics](#)



Recycle Bin



Microsoft Edge



Google Chrome



Finance headline
US Crude Oil Inv...
Search
ENG
2:02 PM
11/13/2025

Step 7) Azure Resources

Azure Resources

The screenshot displays the Microsoft Azure portal interface for a storage account named 'crmstoremlab'. The page title is 'Data protection' and it includes a search bar with the query 'How can I make this storage account resilient?'. The left-hand navigation pane lists various services, with 'Data protection' selected. The main content area is titled 'Data protection provides options for recovering your data when it is erroneously modified or deleted.' and is organized into four sections: Recovery, Tracking, and Access control. The Recovery section includes options for enabling Azure Backup for blobs, point-in-time restore for containers, soft delete for blobs (checked), and soft delete for containers (checked). The Tracking section includes options for enabling versioning for blobs and blob change feed. The Access control section includes an option for enabling version-level immutability support. At the bottom of the page, there are 'Save' and 'Discard' buttons, and a 'Give feedback' link.

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

adm-mh@mhlabcz.onm...
MHLAB (MHLAB.CZ)

Home > crmstoremlab_1781785699797 | Overview > crmstoremlab

crmstoremlab | Data protection ☆

Storage account

How can I make this storage account resilient?

Search

Overview

Activity log

Tags

Diagnose and solve problems

Access Control (IAM)

Data migration

Events

Storage browser

Storage Mover

Partner solutions

Resource visualizer

Data storage

Security + networking

Data management

Storage Actions

Redundancy

Data protection ☆

Object replication

Blob inventory

Static website

Lifecycle management

Azure AI Search

Settings

Monitoring

Data protection provides options for recovering your data when it is erroneously modified or deleted.

Recovery

Enable Azure Backup for blobs

Enable point-in-time restore for containers

Enable soft delete for blobs

Soft delete enables you to recover blobs that were previously marked for deletion, including blobs that were overwritten. [Learn more](#)

Keep deleted blobs for (in days) * 7

Enable soft delete for containers

Soft delete enables you to recover containers that were previously marked for deletion. [Learn more](#)

Keep deleted containers for (in days) * 7

Enable permanent delete for soft deleted items

Tracking

Enable versioning for blobs

Enable blob change feed

Access control

Enable version-level immutability support

Save Discard

Give feedback

Add or remove favorites by pressing Ctrl+Shift+F

Wrap-up

Ideal Sequence of Steps

1. Data exfiltration / backup (checkpoint \$\$\$)
2. Destruction of backups
3. Cutting administrators off from access
4. Encryption of O365 + Azure data
5. Blocking workstations / cache

Impact of an O365 Compromise

Problem	Likelihood	Difficulty of execution	Financial impact
Data exfiltration and extortion	observed	low	low
Encrypted data in O365	we haven't encountered this	medium	medium
Encrypted data in Azure	observed	medium	high
DoS	we have heard about it	low	medium
Wiper	we haven't encountered this	low	high
BEC	common occurrence	low	medium
Abuse of an Azure subscription	observed	low	low

Other impact: <https://www.bleepingcomputer.com/news/security/hackers-use-rmm-tools-to-breach-freighters-and-steal-cargo-shipments/>

What if Microsoft has something up its sleeve?

- » Does Microsoft have unofficial backups?
- » The attackers will find out during the first recovery attempt.
- » This could also be a legal issue (<https://learn.microsoft.com/en-us/compliance/assurance/assurance-data-retention-deletion-and-destruction-overview>)

Defense

- » **Backups** (O365, Azure data, Azure configuration, Entra ID configuration)
- » **Hardening** (tiering, least privilege, separate accounts, PAW)
- » **Monitoring** (XDR, Defender for *)



Thank
《YOU》