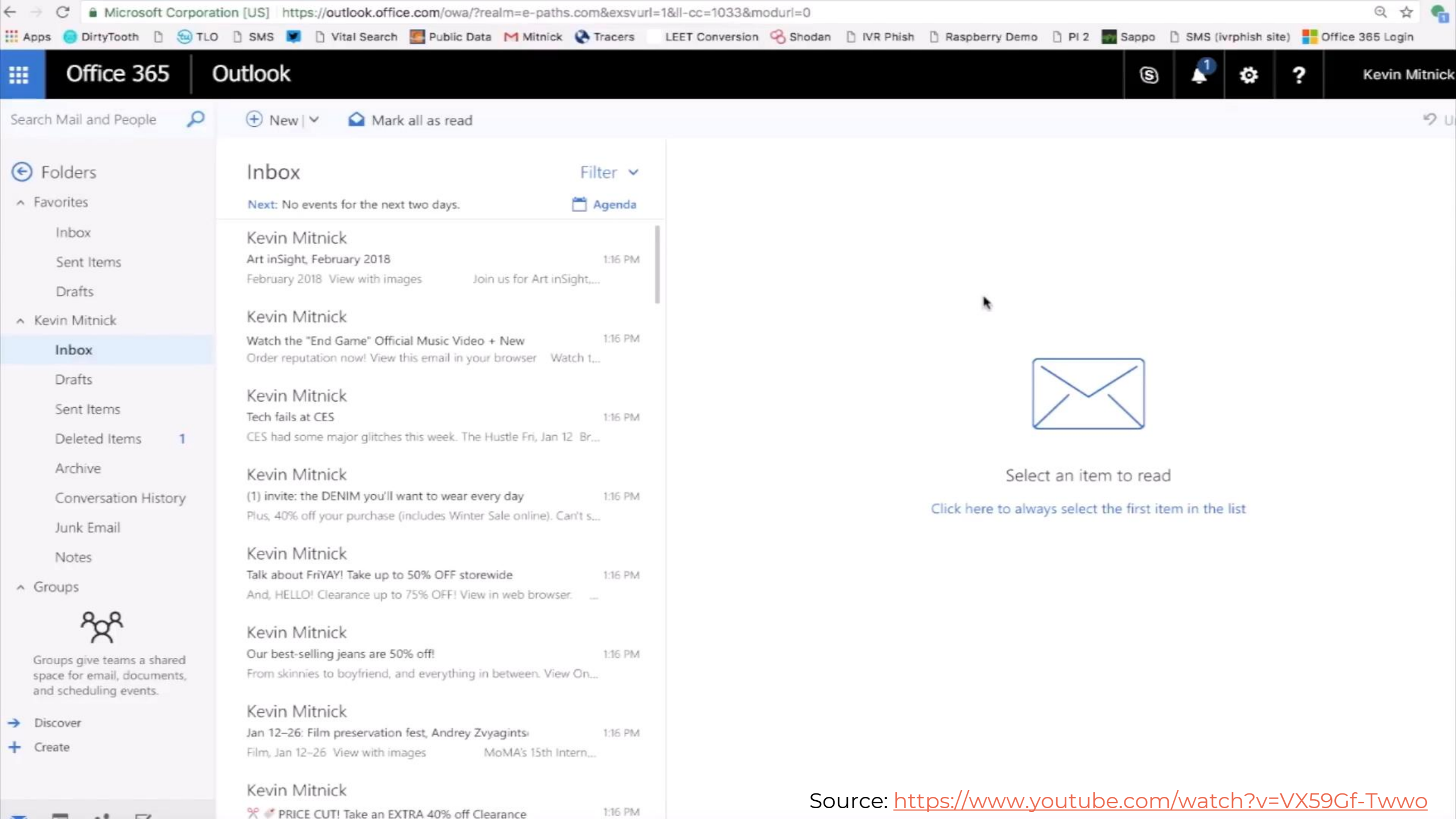
Martin Haller

⟨RansomCloud: Ransomware Operations in Microsoft 365⟩

PATRON⟨IT⟩ OCHRANA A SPRÁVA SÍTÍ



Source: https://www.youtube.com/watch?v=VX59Gf-Twwo

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.

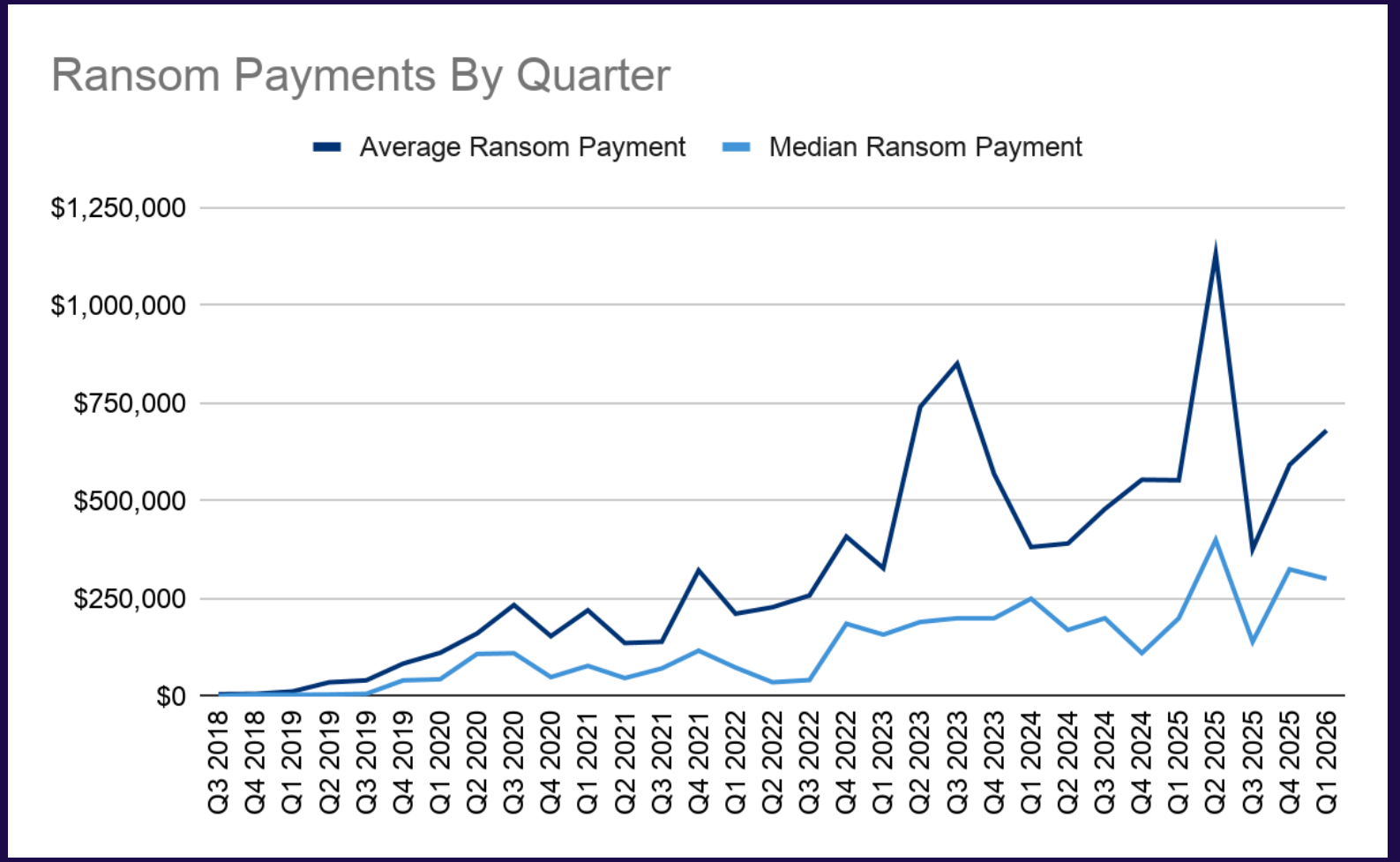
I am, and always will be, on the side of defenders, security professionals, and applicable law.

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)

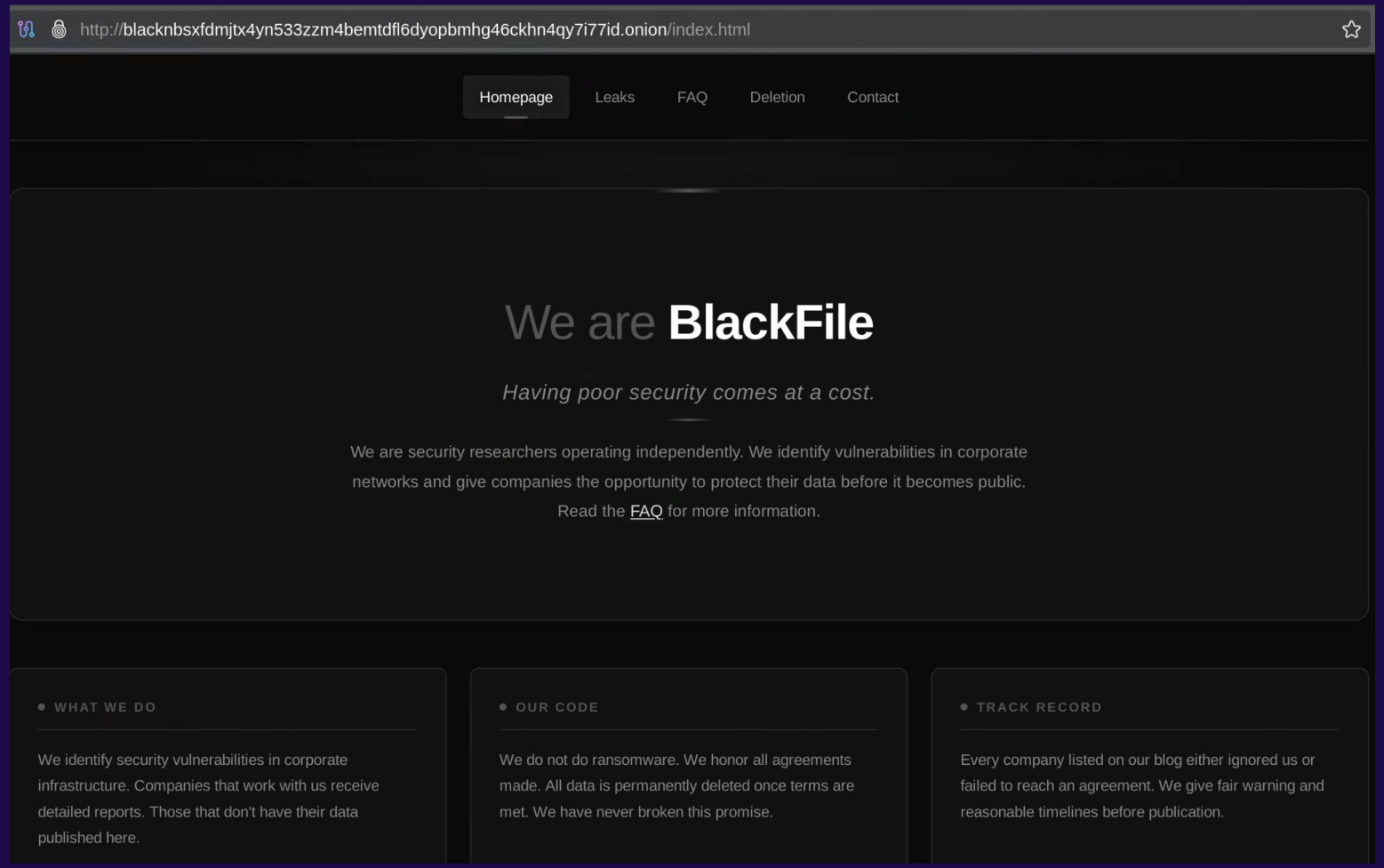
Azure

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

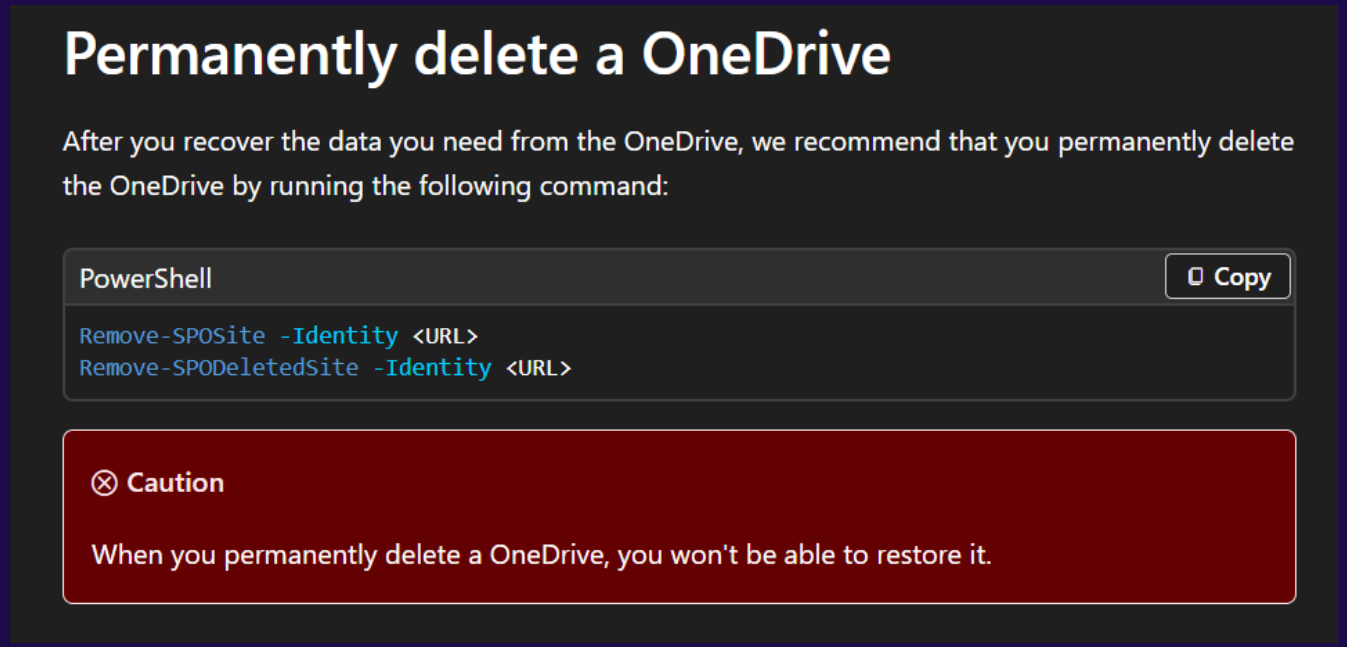
Exchange Online – À la Kevin Mitnick


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

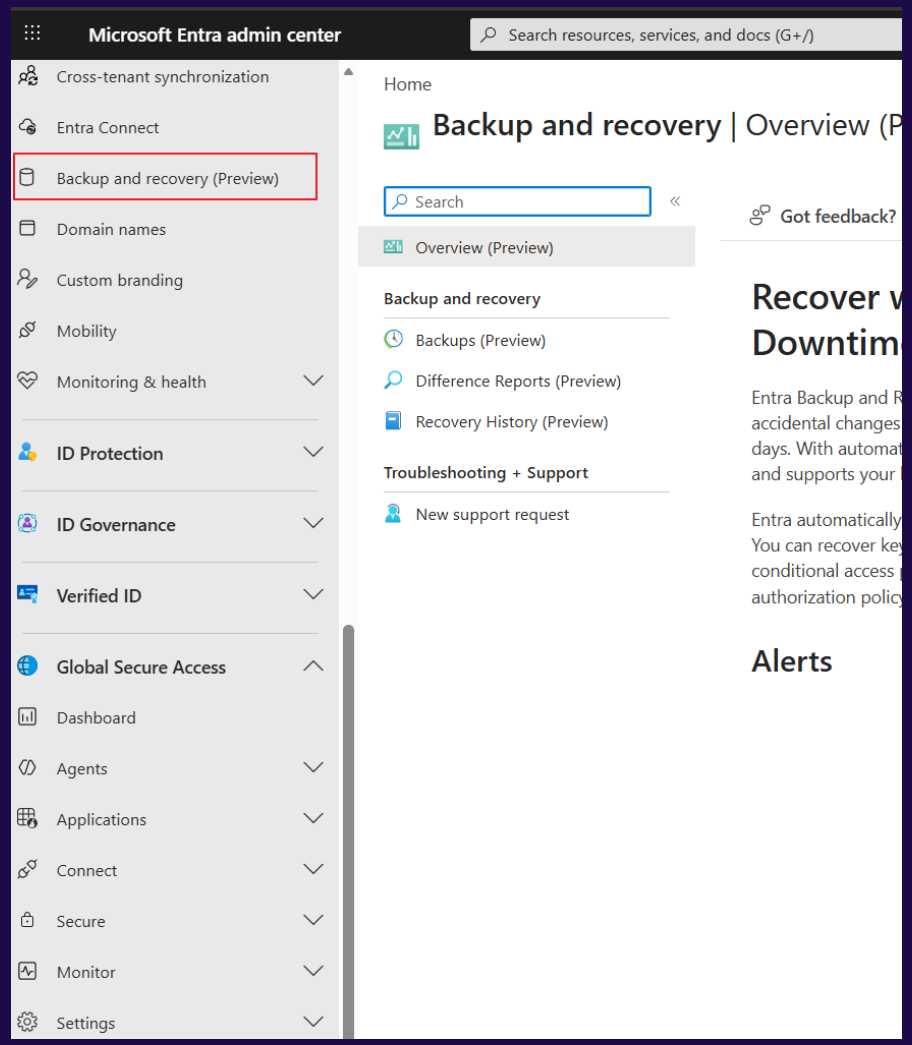
March 16, 2026 03:17 PM 3

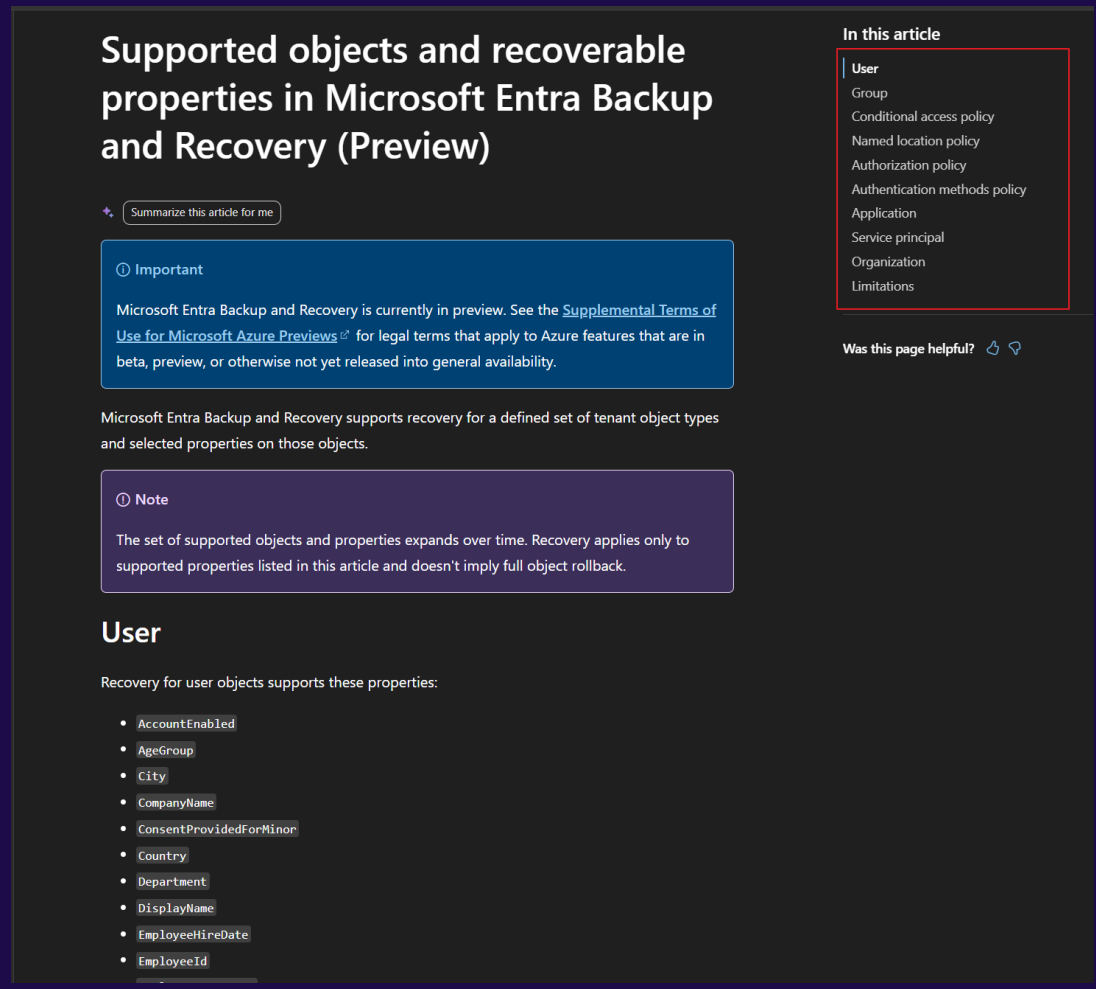
Last week's cyberattack on medical technology giant Stryker was limited to its internal Microsoft environment and remotely wiped tens of thousands of employee devices

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



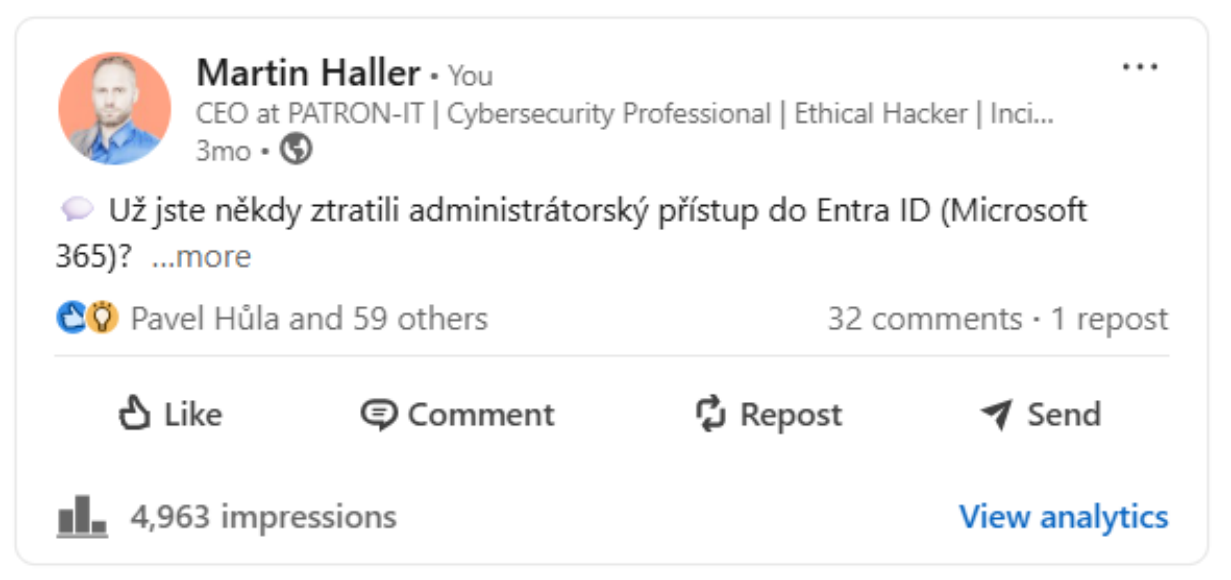


Source: https://learn.microsoft.com/en-us/entra/backup/scope-supported-objects-limitations

Step 6) Blocking Administrators

Blocking Administrators

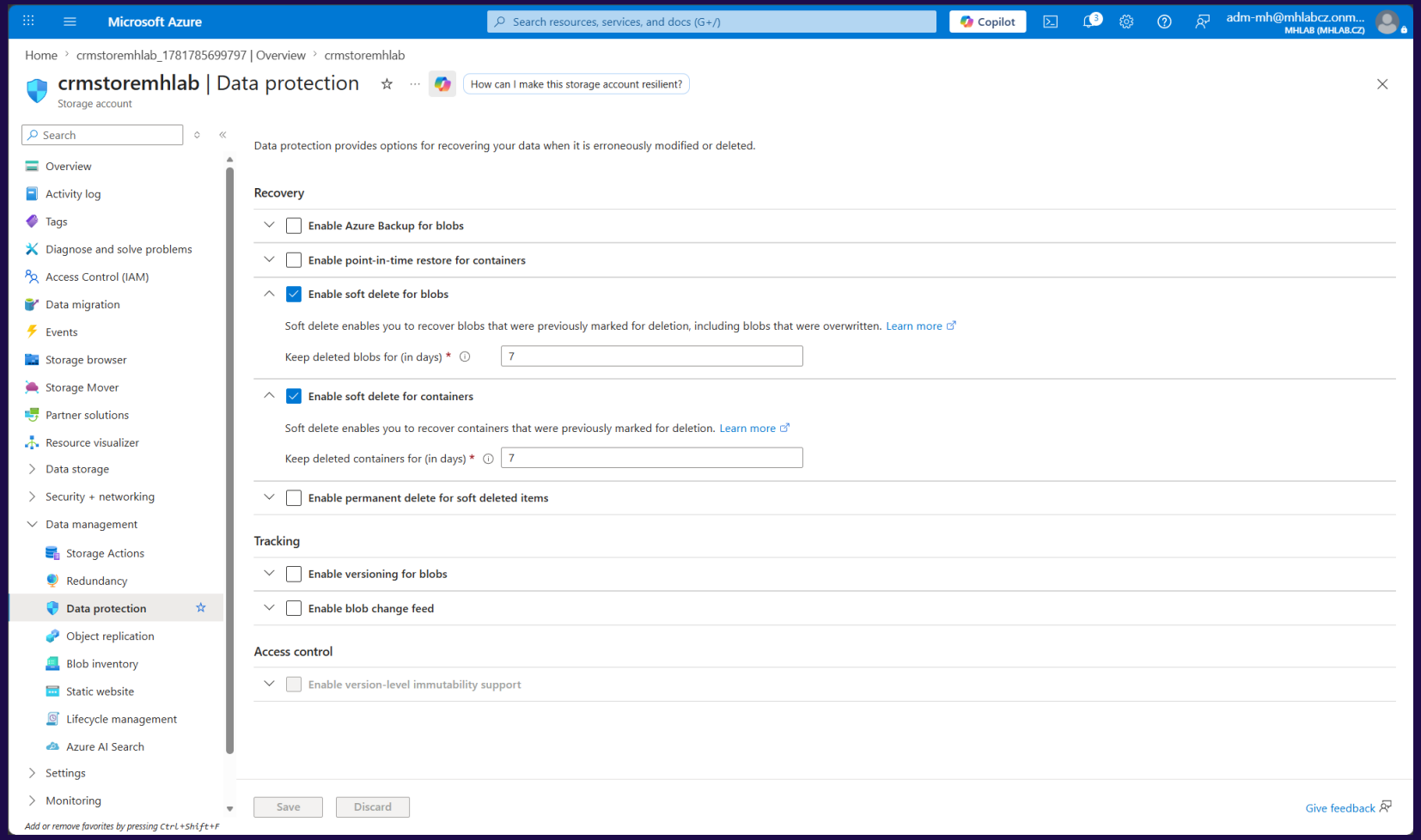
- They need to buy time and have a quiet environment to work.
- A new aspect compared to on-prem ransomware.
- Without support, they won't regain access.




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



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 encoutered this	medium	medium
Encrypted data in Azure	observed	medium	high
DoS	we have heard about it	low	medium
Wiper	we haven't encoutered this	low	high
BEC	common occurence	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⟩