AVANTEC
Competence. Security. Trust.

Weil Sicherheit alles ändert.

Alessandro Salucci (Cyber Security Specialist) salucci@avantec.ch

11. Februar 2026

AVANTEC
Competence. Security. Trust.

```
PDF Editor.exe (0) with command "" connected to https://appsuites.ai/api/update

svchost.exe (3628) created pdf editor.exe (25076) with command: cmd.exe /d /s /c "powershell.exe
"Get-WmiObject Win32_Process | Where-Object { $_.Name -eq 'chrome.exe' }"

svchost.exe (3628) created pdf editor.exe (25076) with command: cmd.exe /d /s /c "powershell.exe
"Get-WmiObject Win32_Process | Where-Object { $_.Name -eq 'msedge.exe' }"

svchost.exe (3628) created pdf editor.exe (25076) with command: cmd.exe /d /s /c "taskkill /IM
chrome.exe"

PDF Editor.exe (25076) created cmd.exe (16036) with command: taskkill /F /IM msedge.exe

pdf editor.exe (25076) with command '"PDF Editor" --cms --partialupdate' connected to
https://appsuites.ai:443
```

We found something weird...

PDF Editor.exe

AppSuite.Ai

It’s just an update…

….or no

AppSuite

Home Terms of Service Privacy Policy DOWNLOAD NOW

Your All-in-One

Productivity Powerhouse

Secure. Private. AI-Powered.

Feeling buried under endless tasks with too little time, space, and the right tools? Juggling multiple apps, struggling with slow software, and worrying about data privacy shouldn’t be part of your daily grind.

AppSuite brings everything you need into one secure, AI-powered platform—so you can focus on getting things done without the stress.

DOWNLOAD NOW

We use essential cookies to make our site work. With your consent, we may also use non-essential cookies to improve user experience, personalize advertisements, and analyze web traffic. For these reasons, we may share your site usage data with our advertising and analytics partners. By clicking “Accept,” you agree to our website’s cookie use as described in our Cookie Policy. You can change your cookie settings at any time by clicking “Preferences.”

Preferences Decline Accept

Why Choose Ap

AVANTEC
Competence. Security. Trust.

11. Februar 2026

Threat Hunting

Before we dive in, let's set the stage:
A modern IT system **is not** a “network.” It's a stack.

AVANTEC
Competence. Security. Trust.

3. Februar 2026

What is Threat Hunting?

What Not..?

AVANTEC
Competence. Security. Trust.

- Threat Hunting ≠ Incident Response
- Threat Hunting ≠ Alert Triage
- Threat Hunting ≠ Threat Intel Feed consumption

Hunting Output

Threat hunting does not end with “we found something.”

AVANTEC
Competence. Security. Trust.

- *New Detection:*
  from TTP → query → signal → rule/use case
- *Telemetry Fix:*
  missing logs, incorrect audit policy, gaps in EDR
- *Control Improvement:*
  hardening / access / segmentation to close observed abuse paths

Cyber Security in Numbers

AVANTEC
Competence. Security. Trust.

241 days
MEAN TIME TO IDENTIFY AND CONTAIN A BREACH
IBM

$4.4M
(CHF 3.5M)
AVERAGE DATA BREACH COST 2025
IBM

43%
OF COMPROMISES GET DETECTED INTERNALLY IN 2024
MANDIANT

26%
AKIRA and LOCKBIT FIRST HALF OF 2025
NCSC

23M
DEVICES INFECTED WORLDWIDE BY THREAT ACTORS (ACROSS *SIX* CONTINENTS) 2025
FLASHPOINT

3.2B+
Stolen Credentials by Threat Actors 2025
FLASHPOINT

Initial Infection Vector

2024 MANDIANT

11. Februar 2026

Offense is Winning

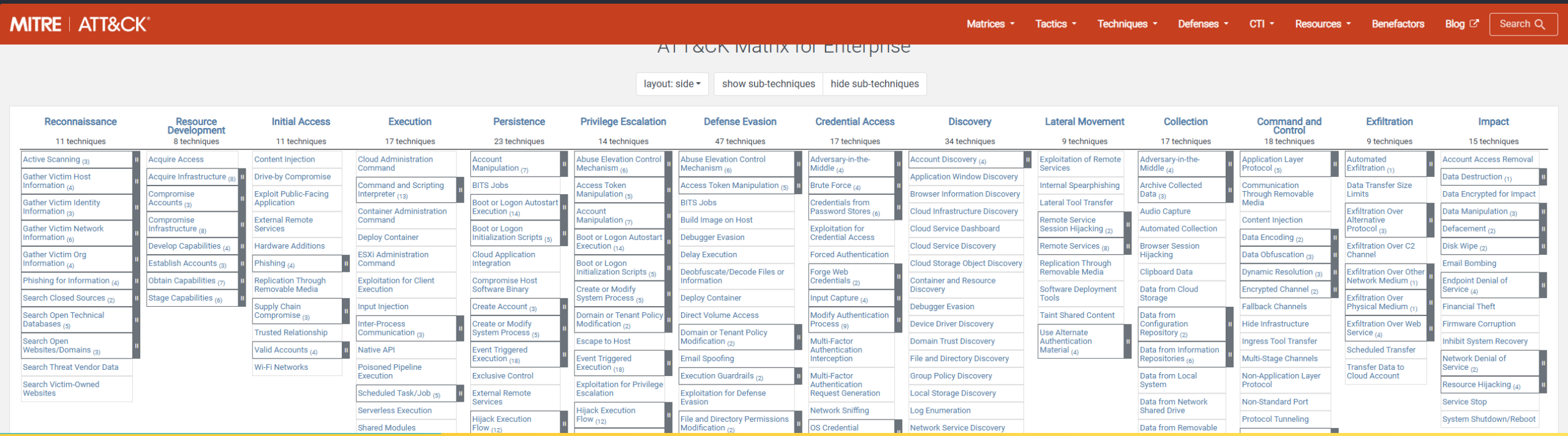
A dollar of offense always wins
against a dollar of defense.

AVANTEC
Competence. Security. Trust.

- **241 Days**
  mean time to identify and contain a breach
- a working idea
- an entry point
- a chain that slips through

MITRE | ATT&CK®
Framework

AVANTEC
Competence. Security. Trust.



https://attack.mitre.org/

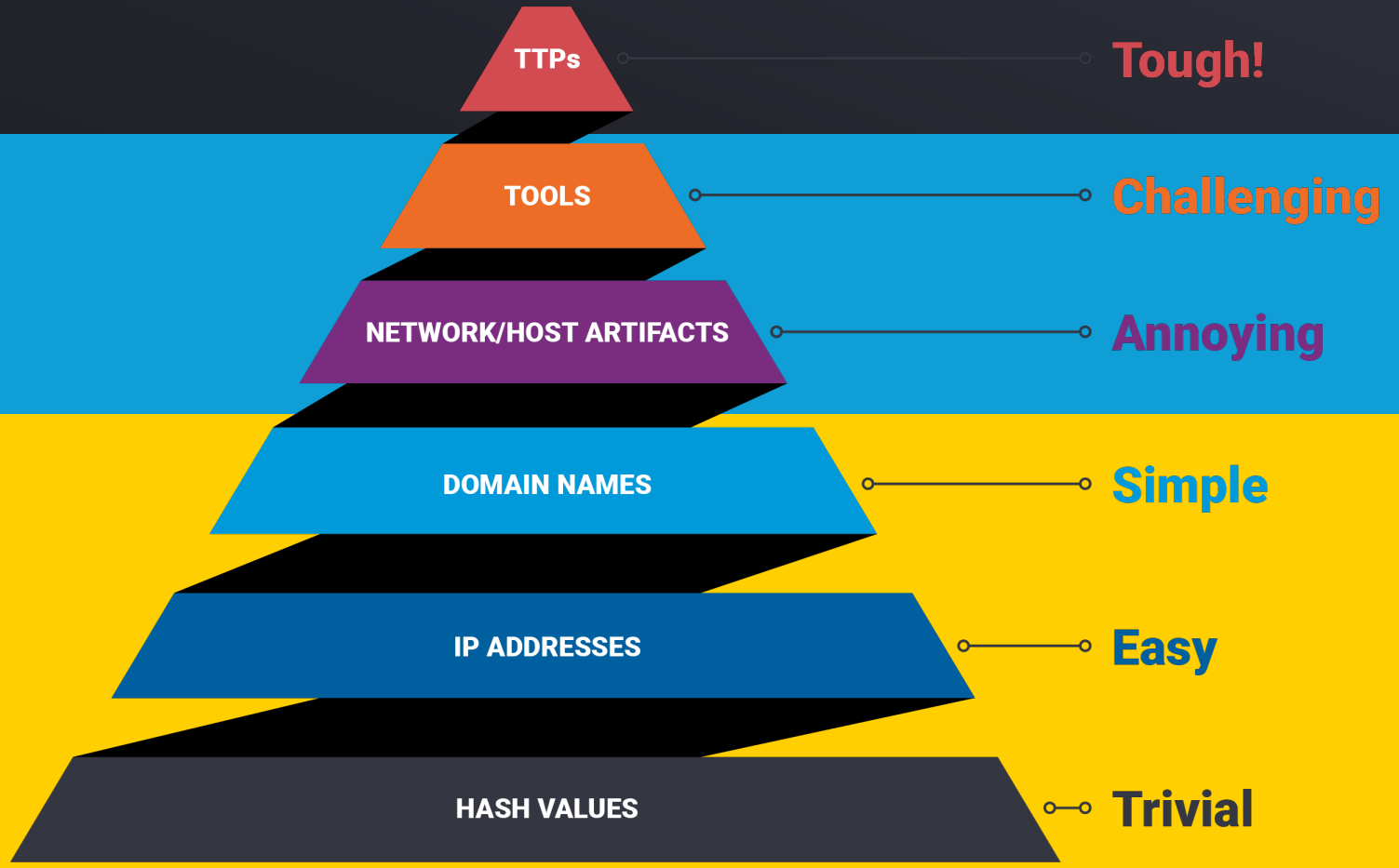
Hunters should be careful...

... about relying too much on IOCs

Pyramid of Pain

Utilize IOCs for quick wins, but attempt to move up the Pyramid of Pain to understand adversary TTPs

AVANTEC
Competence. Security. Trust.



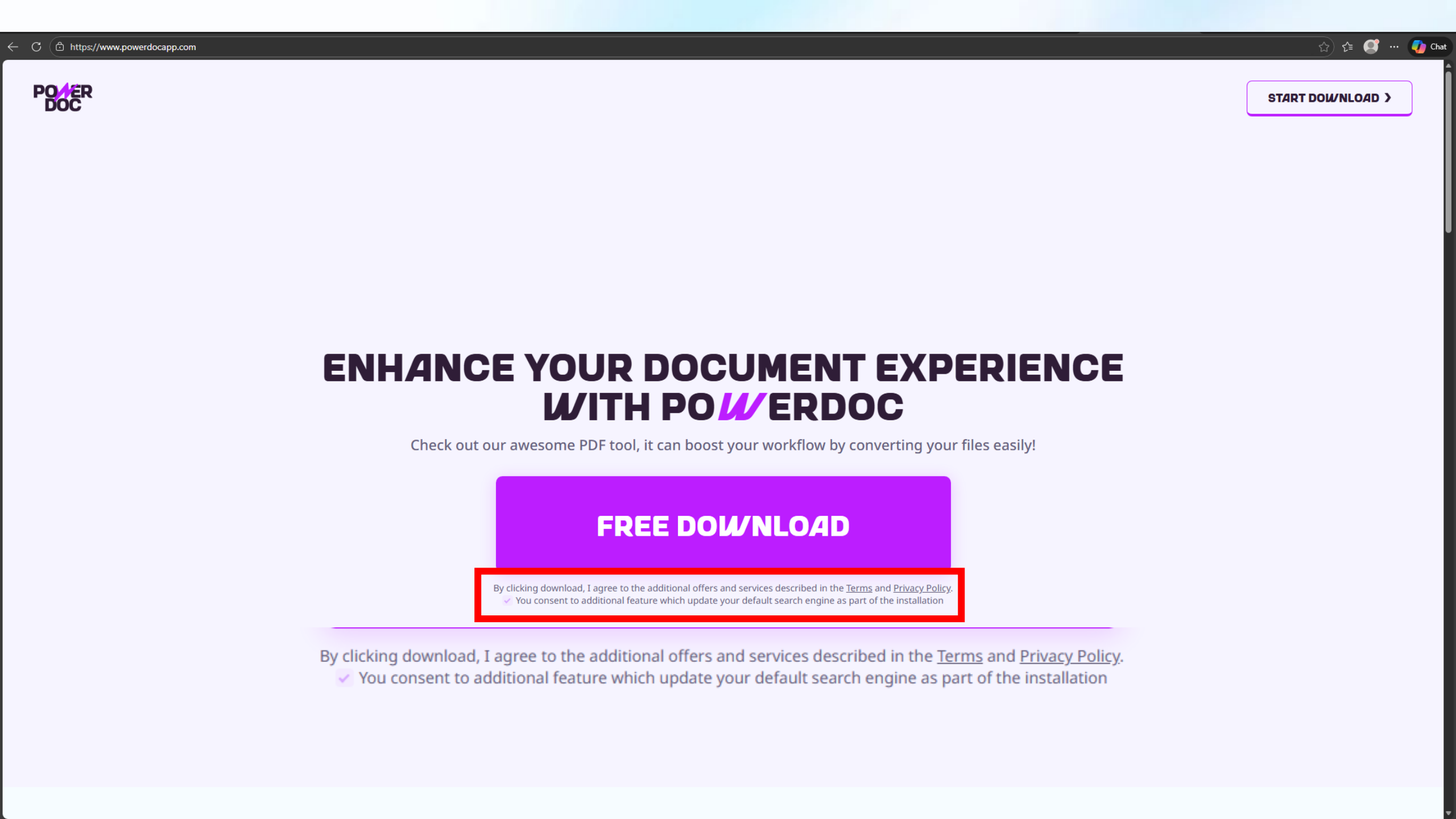
Types of Indicators of Compromise (IoC)

TTPs (Tactics, Techniques, and Procedures) - *Tough*

AVANTEC
Competence. Security. Trust.

- **Tactics, Techniques and Procedures (TTPs)**: How the adversary goes about accomplishing their mission, from reconnaissance all the way through data exfiltration and at every step in between.
- "**Spear phishing**" is a common TTP for establishing a presence in the network. "**Spear phishing with a trojaned PDF file**" or "... **with a link to a malicious .SCR file disguised as a ZIP**" would be more specific versions.
- "**Dumping cached authentication credentials and reusing them in Pass-the-Hash attacks**" would be a TTP. Notice we're not talking about specific tools here, as there are any number of ways of weaponizing a PDF or implementing Pass-the-Hash.

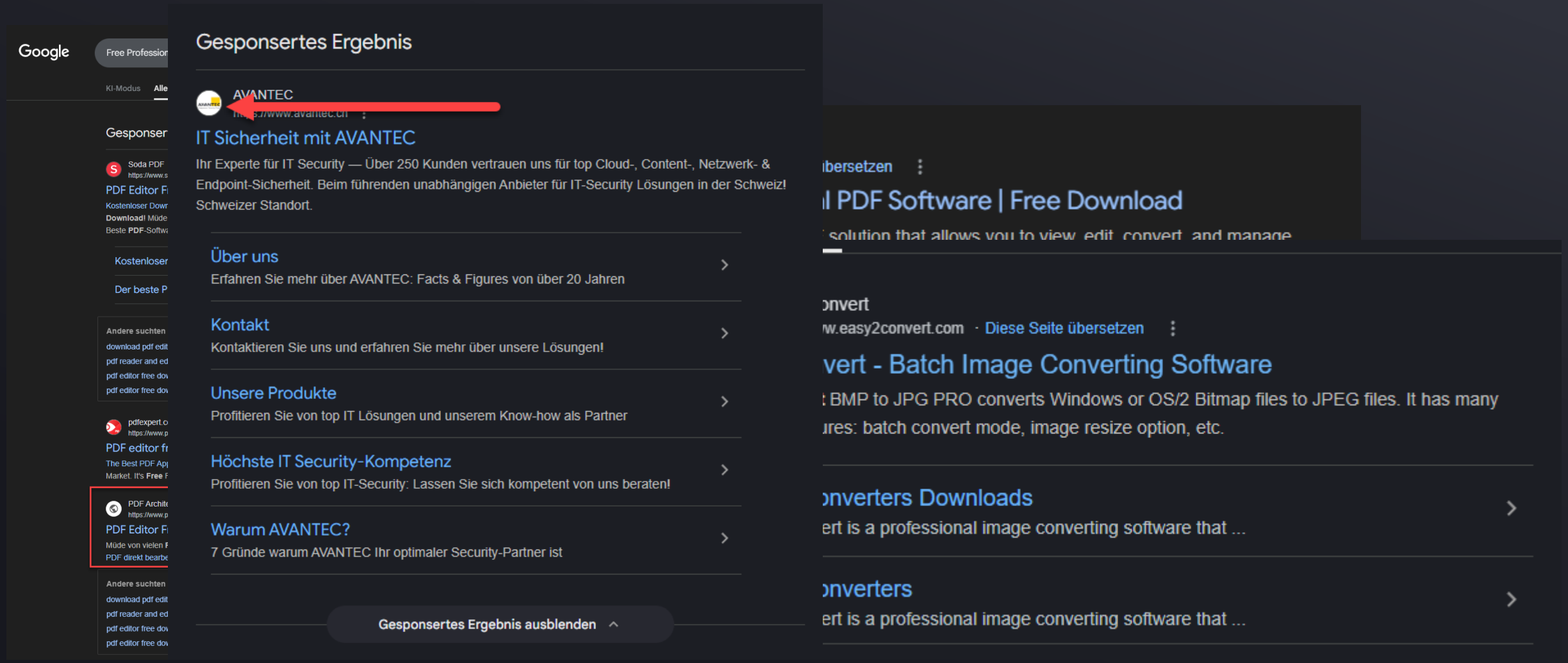
Questions You Should Be Asking Your MSSP


https://www.powerdocapp.com
Chat
POWERDOC
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
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

What do they all have in common?

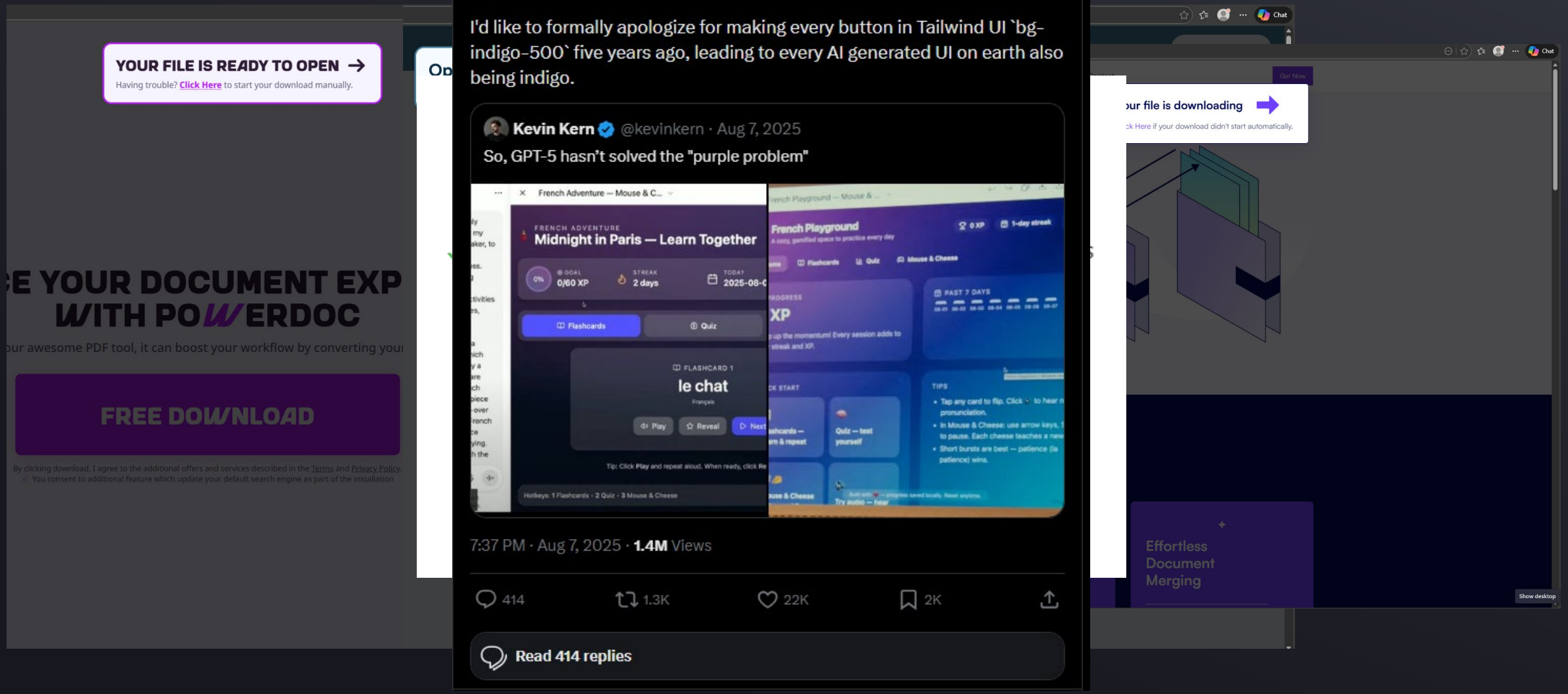
AVANTEC
Competence. Security. Trust.

They all get Advertised over Google



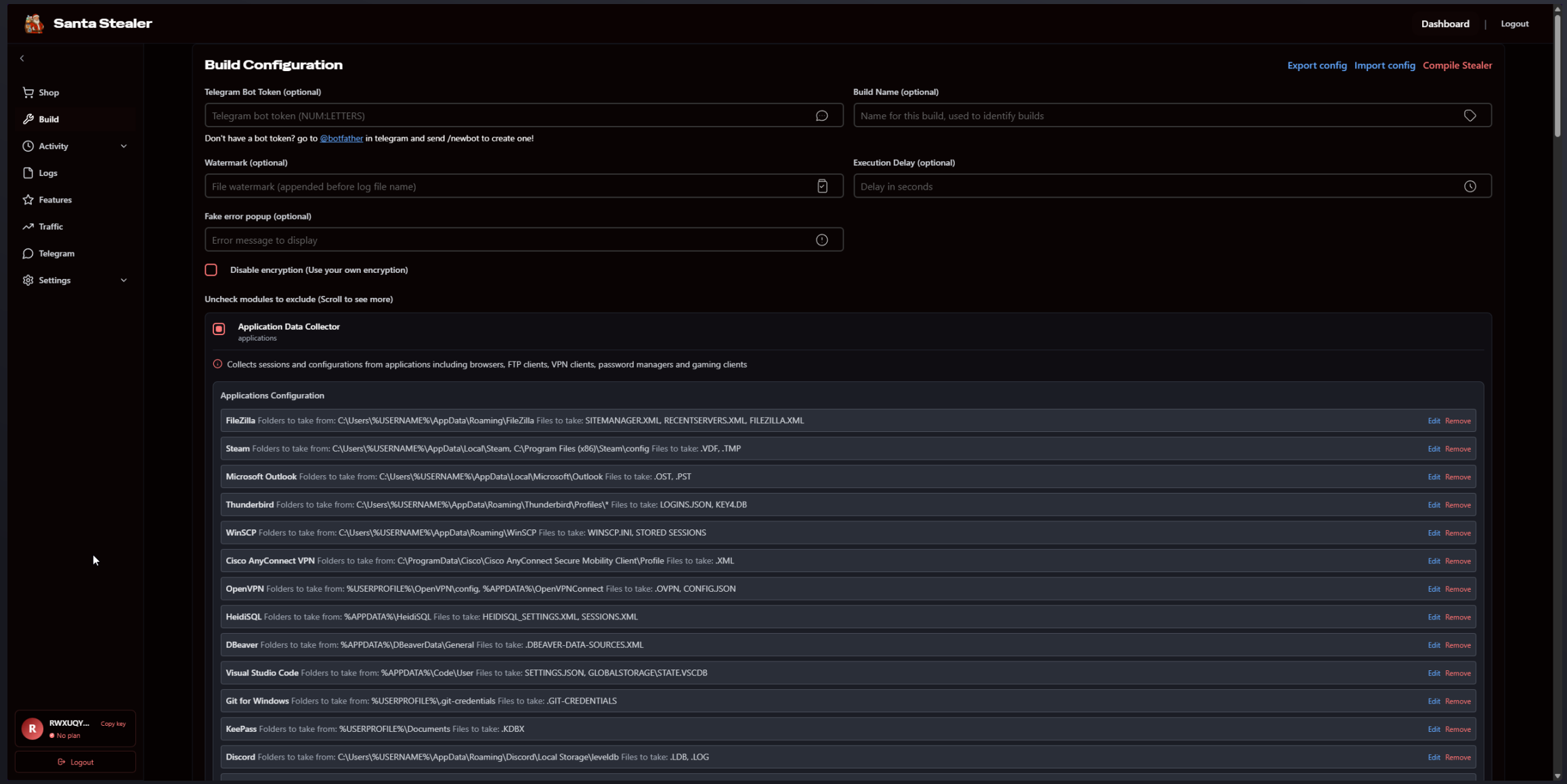
Let’s download them...

AVANTEC
Competence. Security. Trust.



What we know...

AVANTEC
Competence. Security. Trust.



1Password Folders to take from

AnyDesk Folders to take from:

Auto FTP Manager Folders to t

Azure Folders to take from: %U

Collects sessions and configurations from applications including browsers, FTP clients, VPN clients, password managers and gaming clients

Applications Configuration

FileZilla Folders to take from: C:\Users\%USERNAME%\AppData\Roaming\FileZilla Files to take: SITEMANAGER.XML, RECENTSERVERS.XML, FILEZILLA.XML

Steam Folders to take from: C:\Users\%USERNAME%\AppData\Local\Steam, C:\Program Files (x86)\Steam\config Files to take: .VDF, .TMP

E, .DB, .JSON

AVANTEC
Competence. Security. Trust.

Basic Plan

$200 / Month

- ✓ Full Support & Feature Requests
- ✓ Custom Folders
- ✗ Edit File Types
- ✗ Edit Crypto Keywords
- ✗ Edit Execution Delay
- ✓ Favorite Logs
- ✓ Download Previous Builds
- ✓ Unlimited Traffic Tag Changes
- ✗ Polymorphic C Engine
- ✗ File Binding
- ✗ Crypto Clipper
- ✗ Custom Feature Implementation
- ✗ Payload conversion

Purchase Plan

Premium Plan

$300 / Month

- ✓ Full Support & Feature Requests
- ✓ Custom Folders
- ✓ Edit File Types
- ✓ Edit Crypto Keywords
- ✓ Edit Execution Delay
- ✓ Favorite Logs
- ✓ Download Previous Builds
- ✓ Unlimited Traffic Tag Changes
- ✓ Polymorphic C Engine
- ✓ File Binding
- ✓ Crypto Clipper
- ✓ Custom Feature Implementation
- ✓ Payload conversion

Purchase Plan

Lifetime Plan

$1000 / Lifetime

- ✓ Full Support & Feature Requests
- ✓ Custom Folders
- ✓ Edit File Types
- ✓ Edit Crypto Keywords
- ✓ Edit Execution Delay
- ✓ Favorite Logs
- ✓ Download Previous Builds
- ✓ Unlimited Traffic Tag Changes
- ✓ Polymorphic C Engine
- ✓ File Binding
- ✓ Crypto Clipper
- ✓ Custom Feature Implementation
- ✓ Payload conversion

Purchase Plan

TotalCommander Folders to tal

UltraVNC Folders to take from:

Exodus Wallet Folders to take f

Riot Games Folders to take fro

Remote Desktop Folders to take from: %USERPROFILE%\Documents Files to take: .RDP

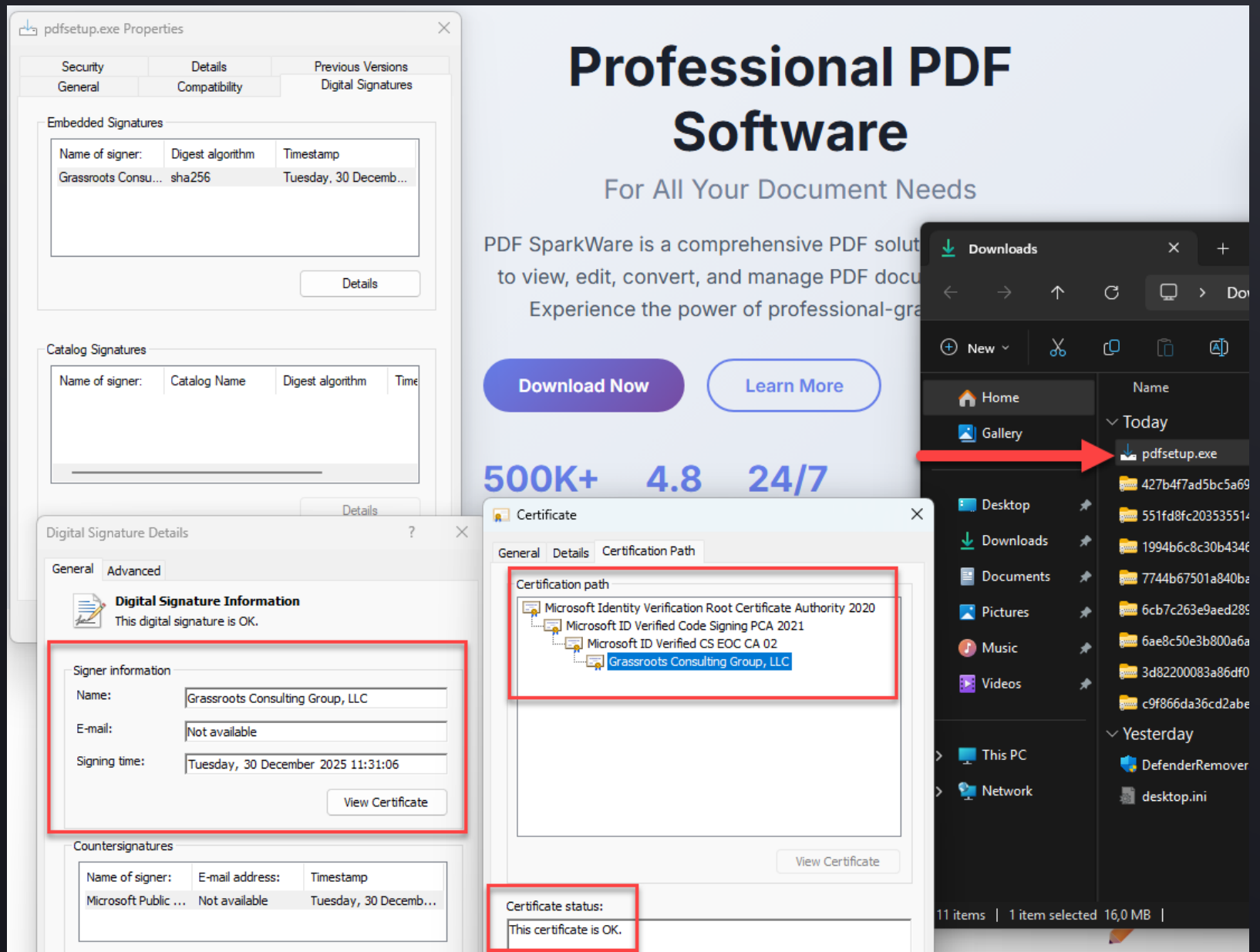
Cyberduck Folders to take from: C:\Users\%USERNAME%\AppData\Roaming\Cyberduck Files to take: BOOKMARKS.PLIST

7-Zip Folders to take from: C:\Users\%USERNAME%\AppData\Roaming\7-Zip Files to take: 7ZFM.INI

Norton Password Manager Folders to take from: C:\Users\%USERNAME%\AppData\Local\Norton Files to take: *

Trusted Signatures as Camouflage

AVANTEC
Competence. Security. Trust.



EvilAI
Malware Campaign

Fake AI Tools

Signed & Stealthy

Malicious Websites & Ads

Global Targets

Data Theft & C2 Control

Deception - Evasion - Exfiltration

MITRE | ATT&CK® Mapping

AVANTEC
Competence. Security. Trust.

PDF Editor.exe

TA0002 Execution

T1059.007 Scripting: JavaScript

Execution of script files via JavaScript

TA0003 Persistence

T1053 Scheduled task/job

Creation of scheduled task to run specified programs at regular intervals

T1547.009 Shortcut modification

Creation of shortcut file for PDF Editor in the Start Menu Programs folder

T1547.001 Registry Run keys/ Startup folder

Addition of an entry to the Run key to automatically execute PDFEditorUpdater at every user logon

TA0007 Discovery

T1057 Process discovery

Query running processes for instances of Microsoft Edge and Google Chrome using WMI

T1518.001 Security software discovery

- Query the Windows Registry for installed security solutions
- Discover uninstall strings or configuration settings that may be used for further automated actions

TA0040 Impact

T1489 Service stop

Termination of browser processes

TA0006 Credential access

T1555 Credentials from password stores

Accessed and copied "Web Data" and "Preferences" files from Microsoft Edge and Google Chrome browser profiles

TA0003 - Persistence

T1053.005 - Creation of scheduled tasks for logon/start/repeating triggers.

AVANTEC
Competence. Security. Trust.

```
#event_simpleName=ProcessRollup2
| ImageFileName=/\\schtasks\.exe$/i
| CommandLine=/\/create/i
| CommandLine=/\/sc\s+(onlogon|onstart|minute|hourly|daily)/i
| CommandLine=/\/ru\s+("?(SYSTEM|LOCAL SERVICE|NETWORK SERVICE)"?)/i
  OR CommandLine=/\/rl\s+highest/i
  OR CommandLine=/\/it\b/i
| regex(field=CommandLine,
regex="(?i)\\/TR\\s+.*?\\\\(Users\\\\[^\\\\]+\\\\(Downloads|Desktop|AppData|Temp)|Windo
ws\\\\Temp|ProgramData|Public)\\\\")
| table([@timestamp, ComputerName, UserName, ParentBaseFileName, CommandLine])
```

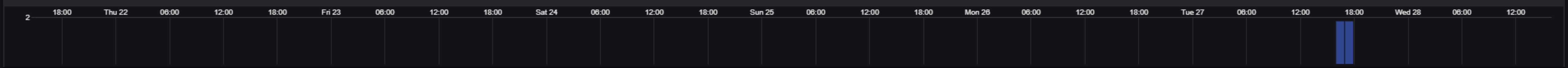
TA0003 - Persistence

T1053.005 - Creation of scheduled tasks for logon/start/repeating triggers.

AVANTEC
Competence. Security. Trust.

Results Events

Save



@timestamp	ComputerName	UserName	ParentBaseFileName	CommandLine
Jan. 27, 2026 17:23:39.444	[redacted]	[redacted]	PDFConverter.exe	schtasks.exe /Create /TN \Microsoft\Windows\PDFConverter\PDFConverterUpdate /TR "\"C:\Users\[redacted]\Downloads\PDFConverter.exe\" --background" /SC ONLOGON /RL HIGHEST /F
Jan. 27, 2026 17:02:12.821	[redacted]	[redacted]	PDFConverter.exe	schtasks.exe /Create /TN \Microsoft\Windows\PDFConverter\PDFConverterUpdate /TR "\"C:\Users\[redacted]\Downloads\PDFConverter.exe\" --background" /SC ONLOGON /RL HIGHEST /F
Jan. 27, 2026 16:24:16.337	[redacted]	[redacted]	PDFConverter.exe	schtasks.exe /Create /TN \Microsoft\Windows\PDFConverter\PDFConverterUpdate /TR "\"C:\Users\[redacted]\Downloads\PDFConverter.exe\" --background" /SC ONLOGON /RL HIGHEST /F
Jan. 27, 2026 16:11:08.769	[redacted]	[redacted]	PDFConverter.exe	schtasks.exe /Create /TN \Microsoft\Windows\PDFConverter\PDFConverterUpdate /TR "\"C:\Users\[redacted]\Downloads\PDFConverter.exe\" --background" /SC ONLOGON /RL HIGHEST /F

ParentBaseFileName	CommandLine
PDFConverter.exe	schtasks.exe /Create /TN \Microsoft\Windows\PDFConverter\PDFConverterUpdate /TR "\"C:\Users\[redacted]\Downloads\PDFConverter.exe\" --background" /SC ONLOGON /RL HIGHEST /F
PDFConverter.exe	schtasks.exe /Create /TN \Microsoft\Windows\PDFConverter\PDFConverterUpdate /TR "\"C:\Users\[redacted]\Downloads\PDFConverter.exe\" --background" /SC ONLOGON /RL HIGHEST /F
PDFConverter.exe	schtasks.exe /Create /TN \Microsoft\Windows\PDFConverter\PDFConverterUpdate /TR "\"C:\Users\[redacted]\Downloads\PDFConverter.exe\" --background" /SC ONLOGON /RL HIGHEST /F
PDFConverter.exe	schtasks.exe /Create /TN \Microsoft\Windows\PDFConverter\PDFConverterUpdate /TR "\"C:\Users\[redacted]\Downloads\PDFConverter.exe\" --background" /SC ONLOGON /RL HIGHEST /F

TA0003 - Persistence

T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

AVANTEC
Competence. Security. Trust.

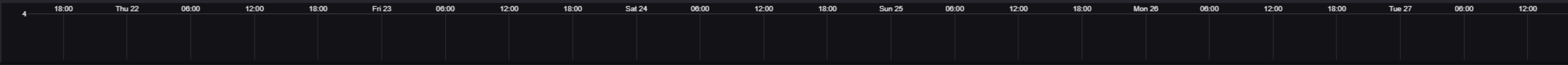
```
#event_simpleName=ProcessRollup2
| ImageFileName=/\\reg\.exe$/i
| CommandLine=/\b(add|delete)\b/i
| CommandLine=/HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run(Once)?/i
| table([@timestamp, ComputerName, UserName, ParentBaseFileName, CommandLine])
```

TA0003 - Persistence

T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

AVANTEC
Competence. Security. Trust.

Results | Events



@timestamp	ComputerName	UserName	ParentBaseFileName	CommandLine
Jan. 27, 2026 17:23:47.841	[redacted]	[redacted]	PDFConverter.exe	reg.exe add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v PDFConverterUpdateHelper /t REG_SZ /d "\"C:\Users\[redacted]\Downloads\PDFConverter.exe\" --helper" /f
Jan. 27, 2026 17:02:40.262	[redacted]	[redacted]	PDFConverter.exe	reg.exe add HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce /v PDFConverterUpdateSetup /t REG_SZ /d "cmd.exe /c \"C:\Users\[redacted]\Downloads\PDFConverter.exe\" --setup" /f
Jan. 27, 2026 17:02:36.880	[redacted]	[redacted]	PDFConverter.exe	reg.exe add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v PDFConverterUpdateHelper /t REG_SZ /d "\"C:\Users\[redacted]\Downloads\PDFConverter.exe\" --helper" /f
Jan. 27, 2026 16:24:22.964	[redacted]	[redacted]	PDFConverter.exe	reg.exe add HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce /v PDFConverterUpdateSetup /t REG_SZ /d "cmd.exe /c \"C:\Users\[redacted]\Downloads\PDFConverter.exe\" --setup" /f
Jan. 27, 2026 16:24:21.075	[redacted]	[redacted]	PDFConverter.exe	reg.exe add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v PDFConverterUpdateHelper /t REG_SZ /d "\"C:\Users\[redacted]\Downloads\PDFConverter.exe\" --helper" /f
Jan. 27, 2026 16:11:15.547	[redacted]	[redacted]	PDFConverter.exe	reg.exe add HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce /v PDFConverterUpdateSetup /t REG_SZ /d "cmd.exe /c \"C:\Users\[redacted]\Downloads\PDFConverter.exe\" --setup" /f
Jan. 27, 2026 16:11:14.552	[redacted]	[redacted]	PDFConverter.exe	reg.exe add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v PDFConverterUpdateHelper /t REG_SZ /d "\"C:\Users\[redacted]\Downloads\PDFConverter.exe\" --helper" /f

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

TA0003 - Persistence

T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

AVANTEC
Competence. Security. Trust.

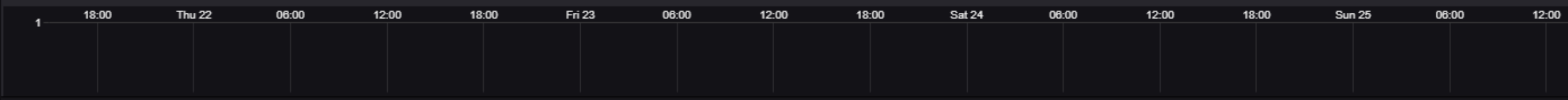
```
#event_simpleName=/File(Create|Write|Rename|Close)/i
| TargetFileName=/\\Microsoft\\Windows\\Start Menu\\Programs\\Startup\\.*\.lnk$/i
| table([@timestamp, ComputerName, TargetFileName])
```

TA0003 - Persistence

T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

AVANTEC
Competence. Security. Trust.

Results | Events



@timestamp	ComputerName	TargetFileName
Jan. 27, 2026 17:02:48.120	[redacted]	\Device\HarddiskVolume3\Users\[redacted]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\PDFConverterPro.lnk
Jan. 27, 2026 16:24:26.848	[redacted]	\Device\HarddiskVolume3\Users\[redacted]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\PDFConverterPro.lnk

TargetFileName

\Device\HarddiskVolume3\Users\[redacted]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\PDFConverterPro.lnk

\Device\HarddiskVolume3\Users\[redacted]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\PDFConverterPro.lnk

MITRE | ATT&CK® Mapping

AVANTEC
Competence. Security. Trust.

PDF Editor.exe

TA0002 Execution

T1059.007 Scripting: JavaScript

Execution of script files via JavaScript

TA0003 Persistence

T1053 Scheduled task/job

Creation of scheduled task to run specified programs at regular intervals

T1547.009 Shortcut modification

Creation of shortcut file for PDF Editor in the Start Menu Programs folder

T1547.001 Registry Run keys/ Startup folder

Addition of an entry to the Run key to automatically execute PDFEditorUpdater at every user logon

TA0007 Discovery

T1057 Process discovery

Query running processes for instances of Microsoft Edge and Google Chrome using WMI

T1518.001 Security software discovery

- Query the Windows Registry for installed security solutions
- Discover uninstall strings or configuration settings that may be used for further automated actions

TA0040 Impact

T1489 Service stop

Termination of browser processes

TA0006 Credential access

T1555 Credentials from password stores

Accessed and copied "Web Data" and "Preferences" files from Microsoft Edge and Google Chrome browser profiles

TA0007 - Discovery

Native Recon Commands (systeminfo / whoami / net / ipconfig / netstat)

AVANTEC
Competence. Security. Trust.

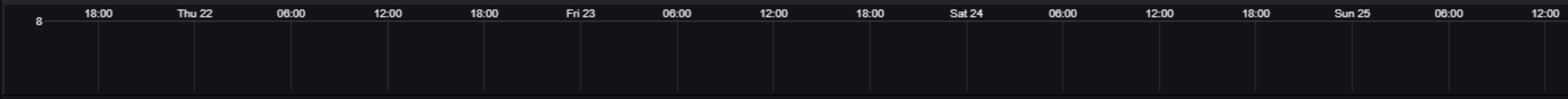
```
#event_simpleName=ProcessRollup2
| ComputerName="REDACTED"
| ImageFileName=/\\(systeminfo|whoami|net|ipconfig|netstat)\.exe$/i
| table([@timestamp, ComputerName, UserName, ParentBaseFileName, ImageFileName,
CommandLine])
```

TA0007 - Discovery

Native Recon Commands (systeminfo / whoami / net / ipconfig / netstat)

AVANTEC
Competence. Security. Trust.

Results | Events



@timestamp	ComputerName	UserName	ParentBaseFileName	ImageFileName	CommandLine
Jan. 27, 2026 17:03:02.326	[redacted]	[redacted]	PDFConverter.exe	\Device\HarddiskVolume3\Windows\System32\NETSTAT.EXE	netstat -ano
Jan. 27, 2026 17:03:00.691	[redacted]	[redacted]	PDFConverter.exe	\Device\HarddiskVolume3\Windows\System32\ipconfig.exe	ipconfig /all
Jan. 27, 2026 17:02:59.157	[redacted]	[redacted]	PDFConverter.exe	\Device\HarddiskVolume3\Windows\System32\net.exe	net localgroup administrators
Jan. 27, 2026 17:02:57.679	[redacted]	[redacted]	PDFConverter.exe	\Device\HarddiskVolume3\Windows\System32\net.exe	net user
Jan. 27, 2026 17:02:56.134	[redacted]	[redacted]	PDFConverter.exe	\Device\HarddiskVolume3\Windows\System32\whoami.exe	whoami /all
Jan. 27, 2026 17:02:49.589	[redacted]	[redacted]	PDFConverter.exe	\Device\HarddiskVolume3\Windows\System32\systeminfo.exe	systeminfo
Jan. 27, 2026 16:24:44.625	[redacted]	[redacted]	PDFConverter.exe	\Device\HarddiskVolume3\Windows\System32\NETSTAT.EXE	netstat -ano
Jan. 27, 2026 16:24:42.952	[redacted]	[redacted]	PDFConverter.exe	\Device\HarddiskVolume3\Windows\System32\ipconfig.exe	ipconfig /all
Jan. 27, 2026 16:24:40.908	[redacted]	[redacted]	PDFConverter.exe	\Device\HarddiskVolume3\Windows\System32\net.exe	net localgroup administrators
Jan. 27, 2026 16:24:37.915	[redacted]	[redacted]	PDFConverter.exe	\Device\HarddiskVolume3\Windows\System32\net.exe	net user
Jan. 27, 2026 16:24:35.174	[redacted]	[redacted]	PDFConverter.exe	\Device\HarddiskVolume3\Windows\System32\whoami.exe	whoami /all
Jan. 27, 2026 16:24:27.841	[redacted]	[redacted]	PDFConverter.exe	\Device\HarddiskVolume3\Windows\System32\systeminfo.exe	systeminfo
Jan. 27, 2026 16:11:20.139	[redacted]	[redacted]	PDFConverter.exe	\Device\HarddiskVolume3\Windows\System32\systeminfo.exe	systeminfo

App execution frequency (global)

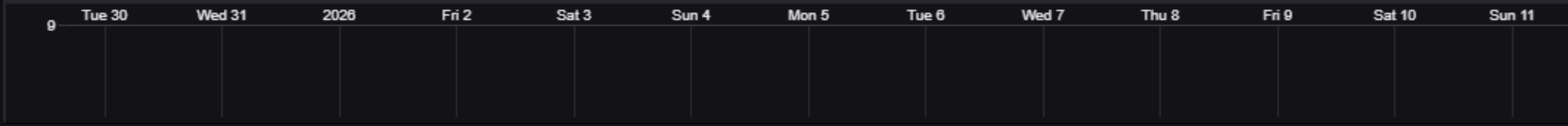
AVANTEC
Competence. Security. Trust.

```
#event_simpleName=ProcessRollup2
| ImageFileName=/PDFConverter\.exe$/i
| groupBy(field=ImageFileName, function=[
    count(as=ExecCount),
    count(field=aid, distinct=true, as=Hosts),
    count(field=UserName, distinct=true, as=Users),
    min(@timestamp, as=FirstSeen),
    max(@timestamp, as=LastSeen)
  ])
| table([ImageFileName, ExecCount, Hosts, Users, FirstSeen, LastSeen], limit=max)
```

App execution frequency (global)

AVANTEC
Competence. Security. Trust.

Results | Events



ImageFileName	ExecCount	Hosts	Users	FirstSeen	LastSeen
\Device\HarddiskVolume3\Users\[redacted]\Downloads\PDFConverter.exe	8	1	1	1769526649939	1769531017905

Mainstay Crypto LLC	BLACK INDIGO LTD	BLUE TAKIN LTD	AMARYLLIS SIGNAL LTD
LONG SOUND LTD	OR KAHOL LTD	TECHNODENIS LTD	SPARROW TIDE LTD
TAU CENTAURI LTD		Grassroots Consulting Group, LLC	

IOCs

If you find one of these certificates in your environment, be sure to contact your MSSP or SOC, or contact us.

Unser Herz

schlägt für Ihre IT-Security.

AVANTEC
Competence. Security. Trust.

Happy Hunting!

Pionier.

IT-Security Anbieter der ersten Stunde seit 1995.

Technisch führend.

Höchste Zertifizierungen, über 5000 erfolgreich durchgeführte Kundenprojekte.

Menschlich verbunden.

Persönliche Betreuung vom Techniker, Account Manager bis hin zum CEO direkt aus Zürich.

Geringe Fluktuation.

Langjährige Mitarbeitende auch im Support. Sie kennen uns und wir kennen Ihre Umgebung.

Marktführende Lösungen.

Wir sind neutral und finden für Sie die marktführende und individuell passende Lösung.

Massgeschneidert.

Angepasst auf Ihre Bedürfnisse – Integration, Managed Services, Cyber Defense Center.