



Weil Sicherheit alles ändert.

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

```
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

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

Why Choose AppSuite

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

Threat Hunting

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



What is Threat Hunting?

What Not..?

- 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.”

- *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



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





Offense is Winning

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

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



ATT&CK Matrix for Enterprise

layout: side ▾ show sub-techniques hide sub-techniques

Reconnaissance 11 techniques	Resource Development 8 techniques	Initial Access 11 techniques	Execution 17 techniques	Persistence 23 techniques	Privilege Escalation 14 techniques	Defense Evasion 47 techniques	Credential Access 17 techniques	Discovery 34 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 15 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (7)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (4)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (4)	Application Layer Protocol (5)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (13)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction (1)
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (7)	Build Image on Host	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Debugger Evasion	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Defacement (2)	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	ESXi Administration Command	Cloud Application Integration	Boot or Logon Initialization Scripts (5)	Delay Execution	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking	Data Obfuscation (3)	Disk Wipe (2)	Defacement (2)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Exploitation for Client Execution	Compromise Host Software Binary	Create or Modify System Process (5)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Email Bombing	Disk Wipe (2)
Search Closed Sources (2)	Obtain Capabilities (7)	Replication Through Removable Media	Input Injection	Event Triggered Execution (18)	Domain or Tenant Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (2)	Endpoint Denial of Service (4)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Inter-Process Communication (3)	Exclusive Control	Escape to Host	Direct Volume Access	Modify Authentication Process (9)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Fallback Channels	Exfiltration Over Physical Medium (1)	Financial Theft
Search Open Websites/Domains (3)		Trusted Relationship	Native API	External Remote Services	Event Triggered Execution (18)	Domain or Tenant Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (6)	Hide Infrastructure	Exfiltration Over Web Service (4)	Firmware Corruption
Search Threat Vendor Data		Valid Accounts (4)	Poisoned Pipeline Execution	External Remote Services	Event Triggered Execution (18)	Event Triggered Execution (18)	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System	Ingress Tool Transfer	Inhibit System Recovery	Inhibit System Recovery
Search Victim-Owned Websites		Wi-Fi Networks	Scheduled Task/Job (5)	Hijack Execution Flow (12)	Exploitation for Privilege Escalation	Exploitation for Privilege Escalation	Network Sniffing	Device Driver Discovery		Data from Network Shared Drive	Multi-Stage Channels	Network Denial of Service (2)	Network Denial of Service (2)
			Serverless Execution	Hijack Execution Flow (12)	Hijack Execution Flow (12)	File and Directory Permissions Modification (2)	OS Credential	Domain Trust Discovery		Data from Removable	Non-Application Layer Protocol	Resource Hijacking (4)	Resource Hijacking (4)
			Shared Modules					File and Directory Discovery			Non-Standard Port	Scheduled Transfer	Service Stop
								File and Directory Permissions Modification (2)			Protocol Tunneling	Transfer Data to Cloud Account	System Shutdown/Reboot

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

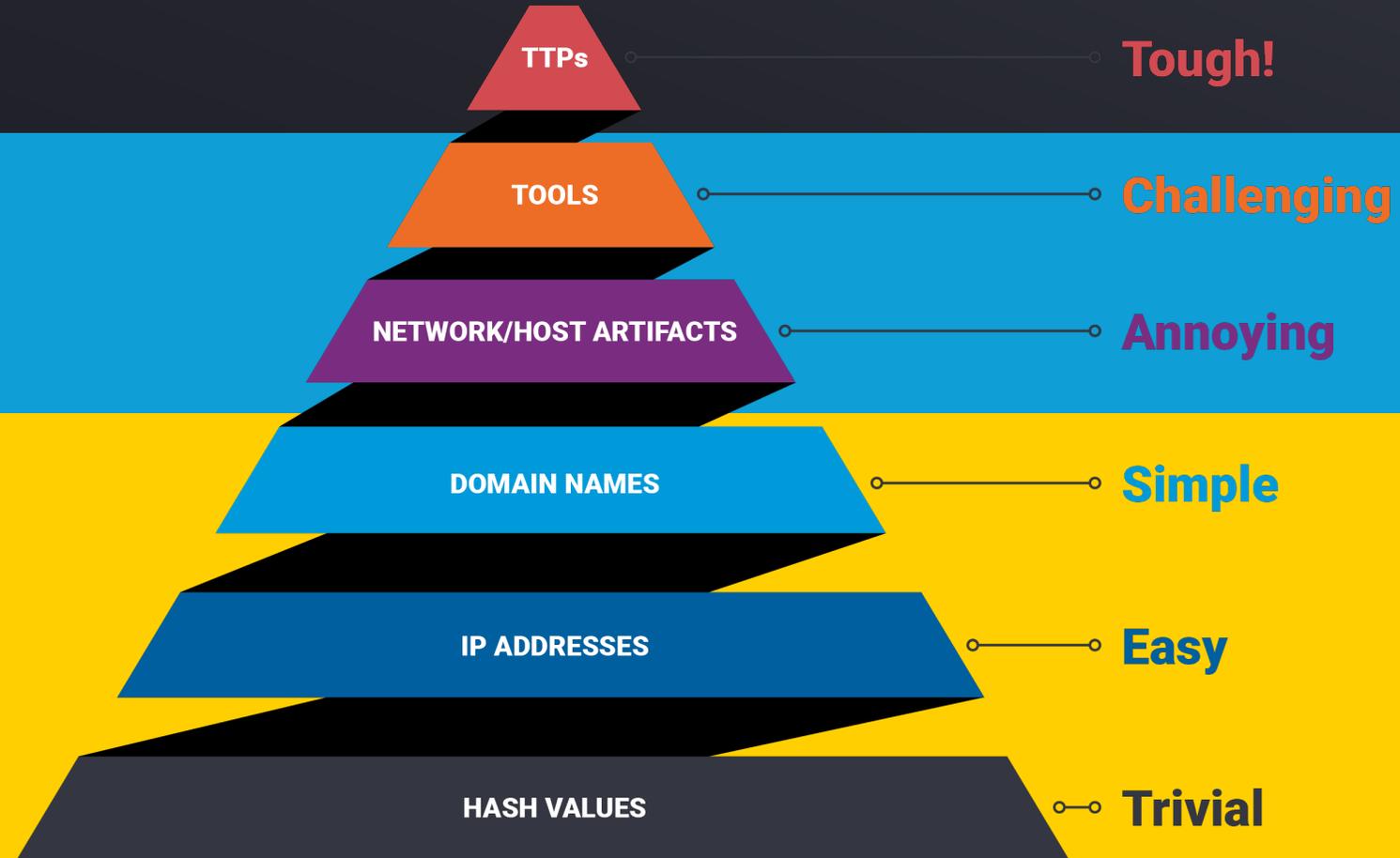
Hunters should be careful...

... about relying too much on IOCs



Pyramid of Pain

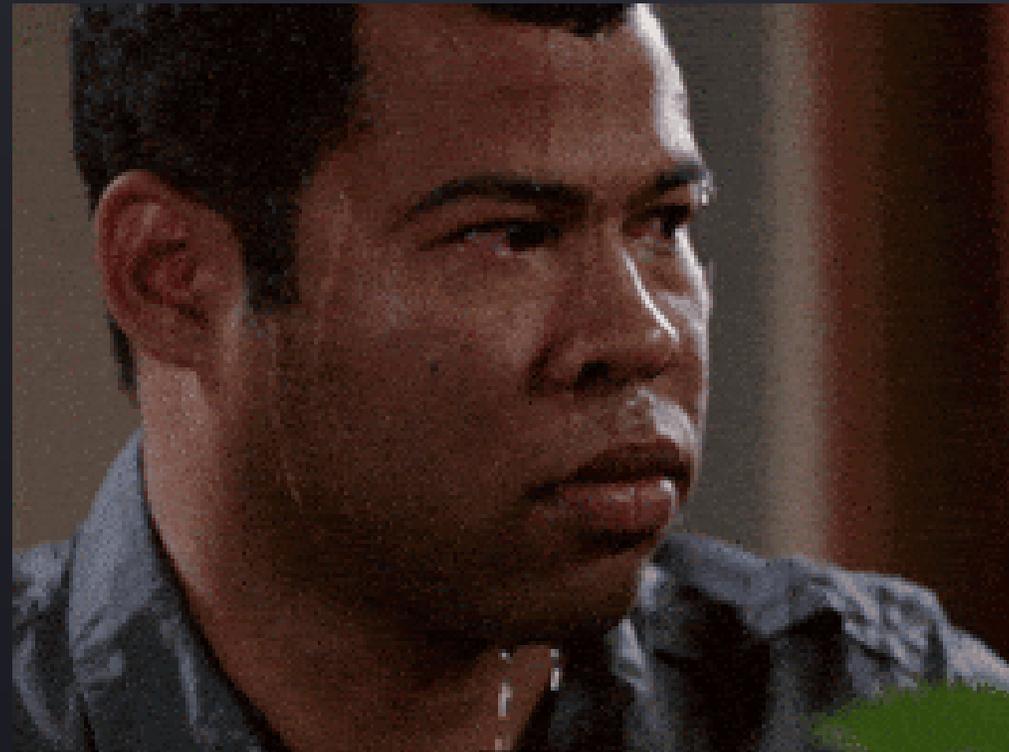
Utilize IOCs for quick wins, but attempt to move up the Pyramid of Pain to understand adversary TTPs



Types of Indicators of Compromise (IoC)

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

- **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



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?

ENHANCE YOUR DOCUMENT EXPERIENCE WITH POW

Check out our awesome PDF tool, it can boost your v

FREE DOWN

PDF Perfectio One Click Aw

Get started for free

By clicking "Get started for free", you accept our [License Agreement](#)

Your All

Proc
Pow

Secure. Priv

Feeling buried un
and the right tool:
software, and wor
your daily grind.

AppSuite brings e
powered platform
without the stress

Professional PDF Software

For All Your Document Needs

PDF SparkWare is a comprehensive PDF solution that allows you
to view, edit, convert, and manage PDF documents with ease.
Experience the power of professional-grade PDF tools.

Download Now

Learn More

500K+
Downloads

4.8
Rating

24/7
Support

DOWNLOAD NOW

Precise.

erDoc

our pdf files.

FREE ⚡

They all get Advertised over Google

Google Free Professor

KI-Modus **Alle**

Gesponser

-  Soda PDF
https://www.sodapdf.com
PDF Editor für Mac & Windows
Kostenlos heruntergeladen! Mehr als 10 Millionen Downloads
Beste PDF-Software
- Kostenlos**
- Der beste PDF-Editor**

Andere suchten

- download pdf editor
- pdf reader and editor
- pdf editor free download
- pdf editor free download

-  pdfexpert.com
https://www.pdfexpert.com
PDF editor für Mac & Windows
The Best PDF App in the Market. It's Free!
-  PDF Architekt
https://www.pdf-architekt.com
PDF Editor für Mac & Windows
Müde von vielen PDF-Editoren? PDF direkt bearbeiten!

Andere suchten

- download pdf editor
- pdf reader and editor
- pdf editor free download
- pdf editor free download

Gesponsertes Ergebnis

 **AVANTEC**
https://www.avantec.ch

IT Sicherheit mit AVANTEC

Ihr Experte für IT Security — Über 250 Kunden vertrauen uns für top Cloud-, Content-, Netzwerk- & Endpoint-Sicherheit. Beim führenden unabhängigen Anbieter für IT-Security Lösungen in der Schweiz! Schweizer Standort.

- Über uns** >
Erfahren Sie mehr über AVANTEC: Facts & Figures von über 20 Jahren
- Kontakt** >
Kontaktieren Sie uns und erfahren Sie mehr über unsere Lösungen!
- Unsere Produkte** >
Profitieren Sie von top IT Lösungen und unserem Know-how als Partner
- Höchste IT Security-Kompetenz** >
Profitieren Sie von top IT-Security: Lassen Sie sich kompetent von uns beraten!
- Warum AVANTEC?** >
7 Gründe warum AVANTEC Ihr optimaler Security-Partner ist

Gesponsertes Ergebnis ausblenden ^

Übersetzen

PDF Software | Free Download

A solution that allows you to view, edit, convert, and manage PDF files.

Convert

www.easy2convert.com · Diese Seite übersetzen

Convert - Batch Image Converting Software

Easy2convert BMP to JPG PRO converts Windows or OS/2 Bitmap files to JPEG files. It has many features: batch convert mode, image resize option, etc.

Converters Downloads

Easy2convert is a professional image converting software that ...

Converters

Easy2convert is a professional image converting software that ...

Let's download them...

YOUR FILE IS READY TO OPEN →

Having trouble? [Click Here](#) to start your download manually.

ACCELERATE YOUR DOCUMENT EXP WITH POWERDOC

With our awesome PDF tool, it can boost your workflow by converting your documents into a searchable format.

FREE DOWNLOAD

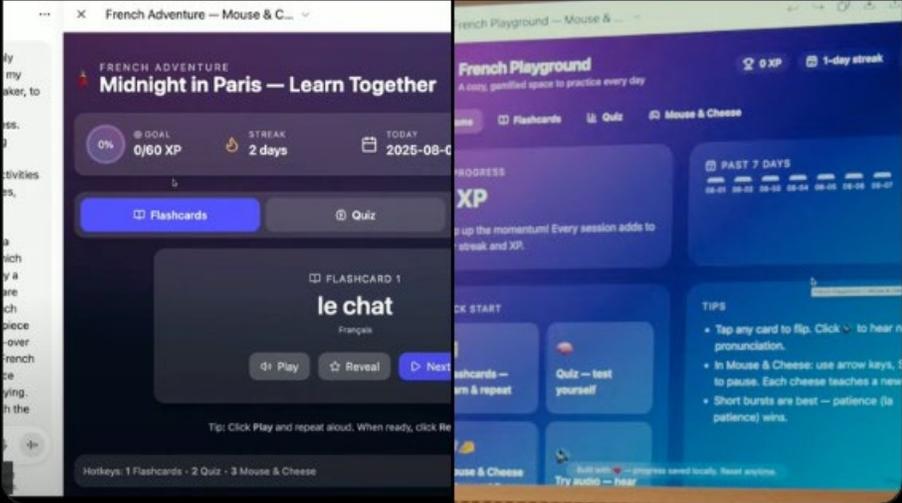
By clicking download, I agree to the additional offers and services described in the [Terms](#) and [Privacy Policy](#).
You consent to additional features which update your default search engine as part of the installation.

← Post

 **Adam Wathan** ✓
@adamwathan

I'd like to formally apologize for making every button in Tailwind UI `bg-indigo-500` five years ago, leading to every AI generated UI on earth also being indigo.

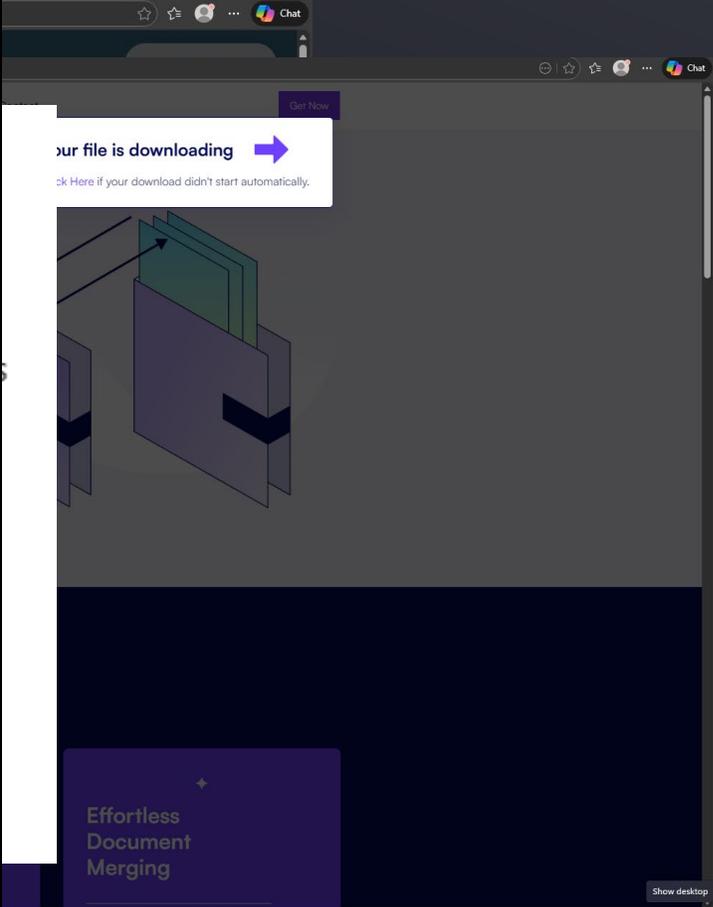
 **Kevin Kern** ✓ @kevinkern · Aug 7, 2025
So, GPT-5 hasn't solved the "purple problem"



7:37 PM · Aug 7, 2025 · 1.4M Views

414 1.3K 22K 2K

Read 414 replies



Get Now

Your file is downloading →

[Click Here](#) if your download didn't start automatically.

Effortless Document Merging

Show desktop

What we know...

Santa Stealer Dashboard Logout

Build Configuration Export config Import config Compile Stealer

Telegram Bot Token (optional)
Telegram bot token (NUM:LETTERS)

Don't have a bot token? go to [@botfather](#) in telegram and send /newbot to create one!

Build Name (optional)
Name for this build, used to identify builds

Watermark (optional)
File watermark (appended before log file name)

Execution Delay (optional)
Delay in seconds

Fake error popup (optional)
Error message to display

Disable encryption (Use your own encryption)

Uncheck modules to exclude (Scroll to see more)

Application Data Collector
applications

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	Edit Remove
Steam Folders to take from: C:\Users\%USERNAME%\AppData\Local\Steam, C:\Program Files (x86)\Steam\config Files to take: .VDF, .TMP	Edit Remove
Microsoft Outlook Folders to take from: C:\Users\%USERNAME%\AppData\Local\Microsoft\Outlook Files to take: .OST, .PST	Edit Remove
Thunderbird Folders to take from: C:\Users\%USERNAME%\AppData\Roaming\Thunderbird\Profiles* Files to take: LOGINS.JSON, KEY4.DB	Edit Remove
WinSCP Folders to take from: C:\Users\%USERNAME%\AppData\Roaming\WinSCP Files to take: WINSCP.INI, STORED_SESSIONS	Edit Remove
Cisco AnyConnect VPN Folders to take from: C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile Files to take: .XML	Edit Remove
OpenVPN Folders to take from: %USERPROFILE%\OpenVPN\config, %APPDATA%\OpenVPN\connect Files to take: .OVPN, CONFIG.JSON	Edit Remove
HeidiSQL Folders to take from: %APPDATA%\HeidiSQL Files to take: HEIDISQL_SETTINGS.XML, SESSIONS.XML	Edit Remove
DBeaver Folders to take from: %APPDATA%\DBeaverData\General Files to take: .DBEAVER-DATA-SOURCES.XML	Edit Remove
Visual Studio Code Folders to take from: %APPDATA%\Code\User Files to take: SETTINGS.JSON, GLOBALSTORAGE\STATE.VSCDB	Edit Remove
Git for Windows Folders to take from: %USERPROFILE%\git-credentials Files to take: .GIT-CREDENTIALS	Edit Remove
KeePass Folders to take from: %USERPROFILE%\Documents Files to take: .KDBX	Edit Remove
Discord Folders to take from: C:\Users\%USERNAME%\AppData\Roaming\Discord\Local Storage\leveldb Files to take: .LDB, .LOG	Edit Remove

RWXUQV... Copy key
No plan

Logout

1Password Folders to take from:

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

AnyDesk Folders to take from:

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

Auto FTP Manager Folders to take from:

Azure Folders to take from: %U

.E, .DB, JSON



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 take from:

UltraVNC Folders to take from:

Exodus Wallet Folders to take from:

Riot Games Folders to take from:

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

Professional PDF Software

For All Your Document Needs

PDF SparkWare is a comprehensive PDF solution to view, edit, convert, and manage PDF documents. Experience the power of professional-grade software.

Download Now

Learn More

500K+ 4.8 24/7

pdfsetup.exe Properties

Security Details Previous Versions
General Compatibility Digital Signatures

Embedded Signatures

Name of signer:	Digest algorithm	Timestamp
Grassroots Consu...	sha256	Tuesday, 30 Decemb...

Details

Catalog Signatures

Name of signer:	Catalog Name	Digest algorithm	Time
-----------------	--------------	------------------	------

Details

Digital Signature Details

General Advanced

Digital Signature Information
This digital signature is OK.

Signer information

Name: Grassroots Consulting Group, LLC

E-mail: Not available

Signing time: Tuesday, 30 December 2025 11:31:06

View Certificate

Countersignatures

Name of signer:	E-mail address:	Timestamp
Microsoft Public ...	Not available	Tuesday, 30 Decemb...

Certificate

General Details Certification Path

Certification path

- Microsoft Identity Verification Root Certificate Authority 2020
 - Microsoft ID Verified Code Signing PCA 2021
 - Microsoft ID Verified CS EOC CA 02
 - Grassroots Consulting Group, LLC

View Certificate

Certificate status:
This certificate is OK.

Downloads

Home Gallery Desktop Downloads Documents Pictures Music Videos This PC Network

Today

- pdfsetup.exe
- 427b47ad5bc5a69
- 551fd8fc203535514
- 1994b6c8c30b434f
- 7744b67501a840ba
- 6cb7c263e9aed28f
- 6ae8c50e3b800a6a
- 3d82200083a86df0
- c9f866da36cd2abe

Yesterday

- DefenderRemover
- desktop.ini

11 items | 1 item selected 16,0 MB

EvilAI

Malware Campaign

Fake AI Tools



Signed & Stealthy



Malicious Websites & Ads



Data Theft & C2 Control



Global Targets



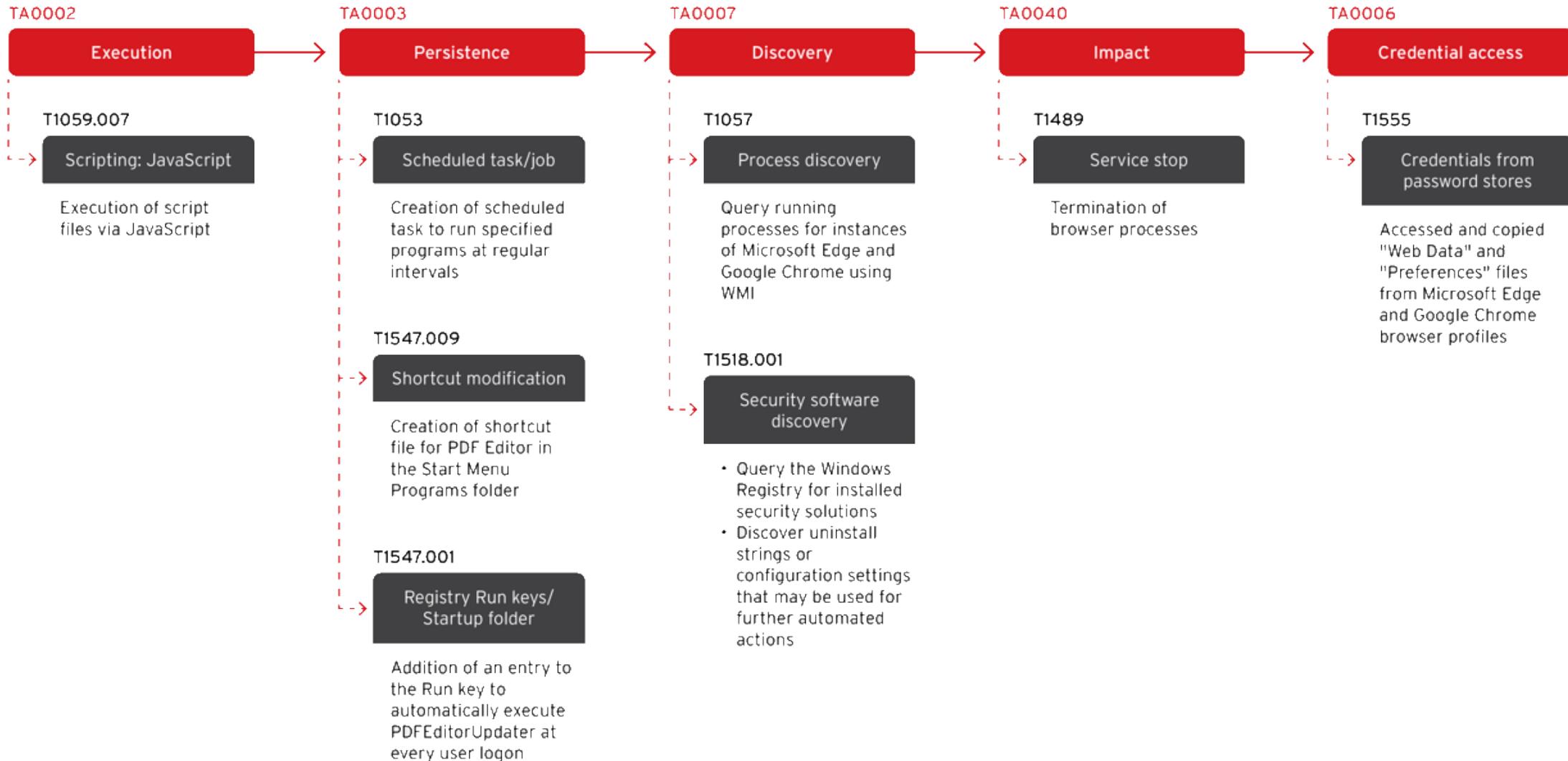
Deception - Evasion - Exfiltration

MITRE | ATT&CK® Mapping



PDF

PDF Editor.exe



TA0003 - Persistence

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

```
#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.

Results		Events		
		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 18:00 Wed 28 06:00 12:00		
2				
@timestamp	ComputerName	UserName	ParentBaseFileName	CommandLine
Jan. 27, 2026 17:23:39.444			PDFConverter.exe	schtasks.exe /Create /TN \Microsoft\Windows\PDFConverter\PDFConverterUpdate /TR "\"C:\Users\ \Downloads\PDFConverter.exe\" --background" /SC ONLOGON /RL HIGHEST /F
Jan. 27, 2026 17:02:12.821			PDFConverter.exe	schtasks.exe /Create /TN \Microsoft\Windows\PDFConverter\PDFConverterUpdate /TR "\"C:\Users\ \Downloads\PDFConverter.exe\" --background" /SC ONLOGON /RL HIGHEST /F
Jan. 27, 2026 16:24:16.337			PDFConverter.exe	schtasks.exe /Create /TN \Microsoft\Windows\PDFConverter\PDFConverterUpdate /TR "\"C:\Users\ \Downloads\PDFConverter.exe\" --background" /SC ONLOGON /RL HIGHEST /F
Jan. 27, 2026 16:11:08.769			PDFConverter.exe	schtasks.exe /Create /TN \Microsoft\Windows\PDFConverter\PDFConverterUpdate /TR "\"C:\Users\ \Downloads\PDFConverter.exe\" --background" /SC ONLOGON /RL HIGHEST /F

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

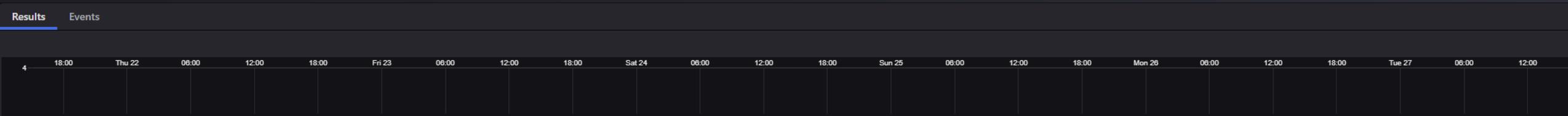
TA0003 - Persistence

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

```
#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



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

TA0003 - Persistence

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

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

TA0003 - Persistence

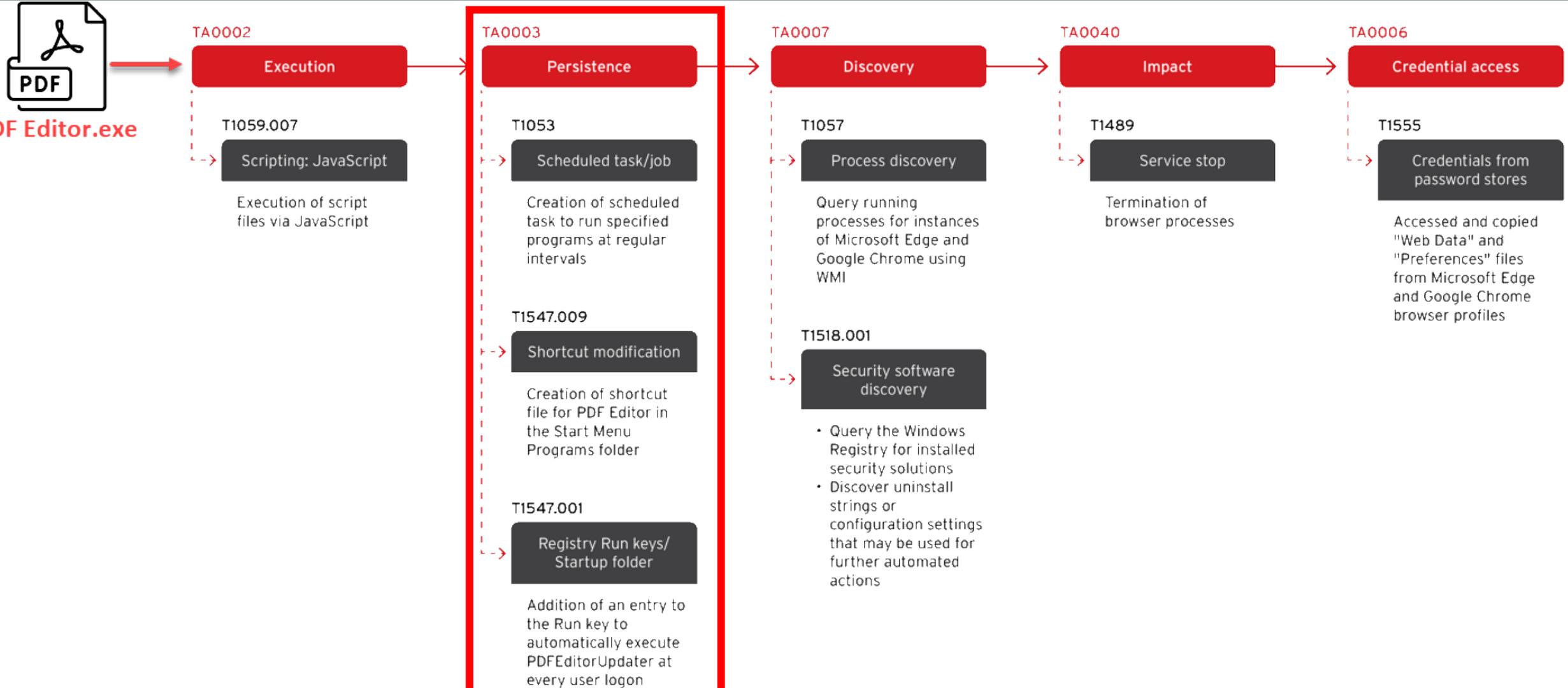
T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder



Results		Events															
		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
:	Jan. 27, 2026 17:02:48.120																
:	Jan. 27, 2026 16:24:26.848																

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



TA0007 - Discovery

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

```
#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)

Results		Events														
		Thu 22		Fri 23		Sat 24		Sun 25								
		18:00	06:00	12:00	18:00	06:00	12:00	18:00	06:00	12:00	18:00	06:00	12:00	18:00	06:00	12:00
		8														
@timestamp	ComputerName	UserName	ParentBaseFileName	ImageFileName	CommandLine											
:	Jan. 27, 2026 17:03:02.326		PDFConverter.exe	\Device\HarddiskVolume3\Windows\System32\NETSTAT.EXE	netstat -ano											
:	Jan. 27, 2026 17:03:00.691		PDFConverter.exe	\Device\HarddiskVolume3\Windows\System32\ipconfig.exe	ipconfig /all											
:	Jan. 27, 2026 17:02:59.157		PDFConverter.exe	\Device\HarddiskVolume3\Windows\System32\net.exe	net localgroup administrators											
:	Jan. 27, 2026 17:02:57.679		PDFConverter.exe	\Device\HarddiskVolume3\Windows\System32\net.exe	net user											
:	Jan. 27, 2026 17:02:56.134		PDFConverter.exe	\Device\HarddiskVolume3\Windows\System32\whoami.exe	whoami /all											
:	Jan. 27, 2026 17:02:49.589		PDFConverter.exe	\Device\HarddiskVolume3\Windows\System32\systeminfo.exe	systeminfo											
:	Jan. 27, 2026 16:24:44.625		PDFConverter.exe	\Device\HarddiskVolume3\Windows\System32\NETSTAT.EXE	netstat -ano											
:	Jan. 27, 2026 16:24:42.952		PDFConverter.exe	\Device\HarddiskVolume3\Windows\System32\ipconfig.exe	ipconfig /all											
:	Jan. 27, 2026 16:24:40.908		PDFConverter.exe	\Device\HarddiskVolume3\Windows\System32\net.exe	net localgroup administrators											
:	Jan. 27, 2026 16:24:37.915		PDFConverter.exe	\Device\HarddiskVolume3\Windows\System32\net.exe	net user											
:	Jan. 27, 2026 16:24:35.174		PDFConverter.exe	\Device\HarddiskVolume3\Windows\System32\whoami.exe	whoami /all											
:	Jan. 27, 2026 16:24:27.841		PDFConverter.exe	\Device\HarddiskVolume3\Windows\System32\systeminfo.exe	systeminfo											
:	Jan. 27, 2026 16:11:20.139		PDFConverter.exe	\Device\HarddiskVolume3\Windows\System32\systeminfo.exe	systeminfo											

App execution frequency (global)

```
#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)

Results Events

g	Tue 30	Wed 31	2026	Fri 2	Sat 3	Sun 4	Mon 5	Tue 6	Wed 7	Thu 8	Fri 9	Sat 10	Sun 11

ImageFileName	ExecCount	Hosts	Users	FirstSeen	LastSeen
\Device\HarddiskVolume3\Users\██████████\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.

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.