Ihre IT.
Heute. Für morgen.

controlware

Beyond Potentially Unwanted Apps

Malware Behind Fake PDF Converters

Version
1.2 – 12-04-2025

Author
Serkan Sirmaci, Cyber Security Analyst @ Controlware CSIRT

Contact
threatreport@controlware.de



Table of Contents

INTRODUCTION 4

HOW DID IT START 4

TECHNICAL OVERVIEW 5

THREAT INTELLIGENCE FINDINGS 11

POSSIBLE HUNTING APPROACHES 18

FINAL ASSESSMENT 21

RECOMMENDED MITIGATION MEASURES 21

IOCS 22

Dear Readers,

PDF converters are among the most frequently searched tools in search engines. The most common use cases are converting PDF files to Word, Word to PDF, or merging several PDFs. Attackers actively exploit this popularity. PDF tools appear harmless, solve everyday problems, and are intentionally searched for by users. This creates a situation where users willingly download and execute installers or use online converters without being suspicious. These fake online converter websites and supposedly trustworthy installers then serve as an initial access point for various types of malwares, which can silently embed themselves into the system and often become active only weeks later.

In recent campaigns, attackers combine several techniques to remain undetected. They use SEO manipulation, typo squatting (registering domains that look almost identical to legitimate ones), and malvertising (purchasing online ads that redirect users to malicious sites) to push their fake services to the top of search results.

Introduction

In recent months, during our threat-hunting activities, we have noticed a new distribution trend involving “PDF Converter” themed software. These tools are delivered through Google ads or SEO poisoning and appear to offer a simple free file conversion service to users. However, many of these samples contain Adware/PUA or beyond a PAU features. Distributors make these tools seem legitimate by using modern user interface, fake reviews, and positive user comments, which makes this trend even more risky. Tools had abused code-signing certificates to look more trustworthy and to bypass SmartScreen, but in most cases the certificates are already revoked. In this write-up, we reviewed the technical features of these campaigns, the strategies used to deceive users, and the security risks they pose.

How did it start

As the Controlware CSIRT, we first detected the active distribution of several PDF Converter tools, likely connected to each other, through EDR systems in October 2025. The initial alert was triggered by a tool named CrystalPDF, which had been added to MalwareBazaar by Karsten Hahn. He also shared his partial analysis of this sample on X

In the following days, we began receiving similar alerts for several other PDF converter tools. We launched a hunting activity to determine whether they were present across our customer environments. This search revealed many matches, which led us to investigate them in more detail. Our goal was to understand how dangerous they might be, to determine whether there was any relationship between the different samples and to identify what kind of hunting strategy could be used to detect these tools effectively. We selected six different PDF converters for further analysis.

Technical overview

We have observed following notable suspicious indicators during our analysis:

(1) Many of the analyzed tools maintain persistence by creating a scheduled task.

- *"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\ConvertMateTask"*
- *"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\Crystal_updater"*
- *"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\Easy2ConvertTask"*
- *"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT \CurrentVersion\Schedule\TaskCache\Tree\PDC_Update"*

This task runs a .NET executable dropped in folder under AppData\Local (Figure 1) during installation, usually named to resemble a legitimate updater.

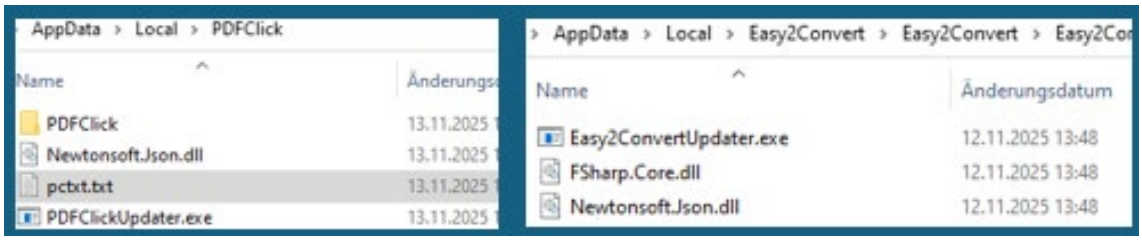


Figure 1 Controlware CSIRT-AppData Folder

Through this task, the software establishes regular connections to remote servers using a recurring pattern of infrastructure. The same directory also contains a dropped text file (Figure 1), which appears to store a UUID used during these network communications.

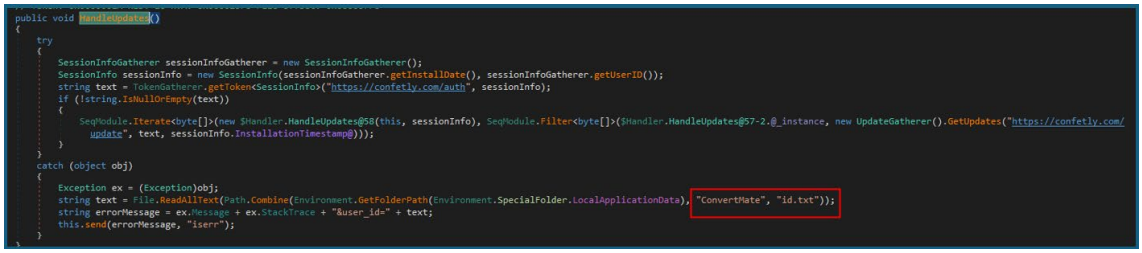


Figure 2 Controlware CSIRT-dnSpy

The traffic is sent in JSON format and protected with AES encryption (Figure 3). Most of the contacted domains are already marked as suspicious by several security vendors on VirusTotal.

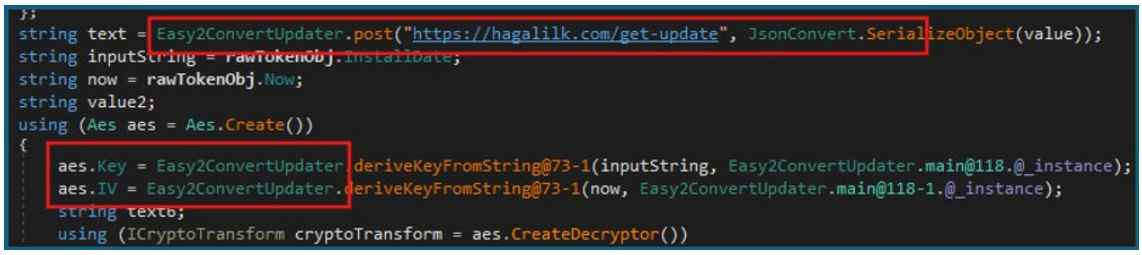


Figure 3 Controlware CSIRT-dnSpy

(2) Most of their certificates have been revoked by the issuer (Figure 4). It appears that when their certificates are revoked, the threat actors switch to a new code-signing certificate.

CrystalPDF and PDFSpark are examples of this behavior.

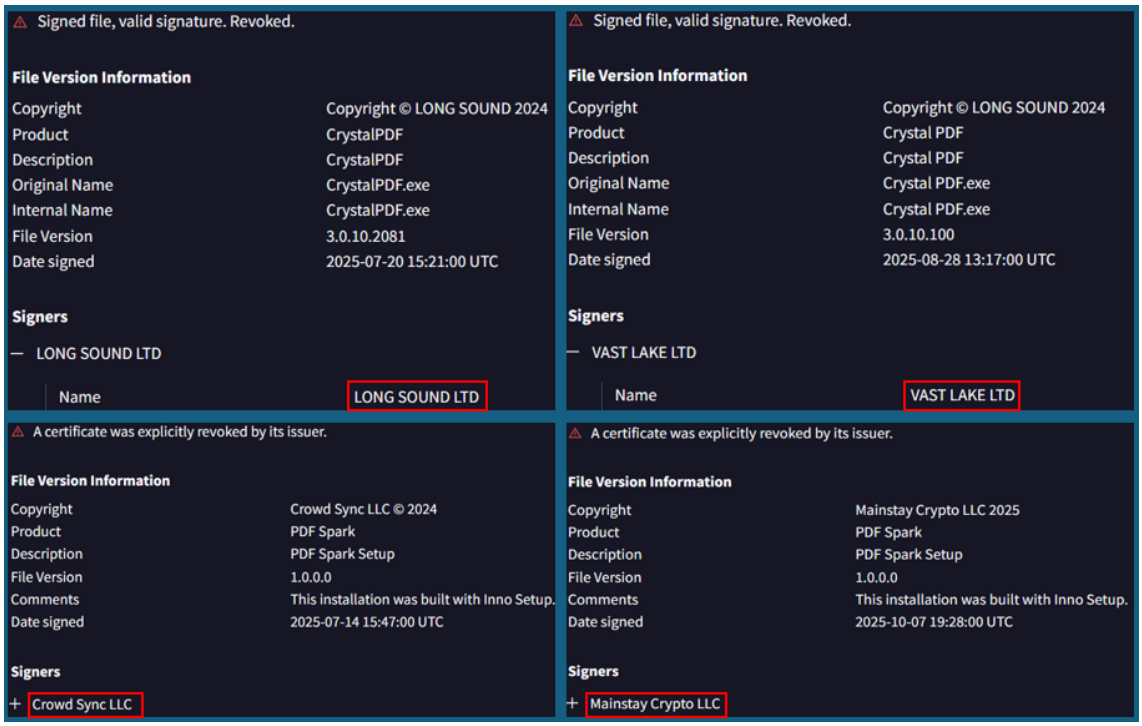


Figure 4 Virus Total

(3) Uninstall options are fake, it removes only the shortcuts and the uninstall registry keys and connects to a domain to show “Good by” but the malware continues to run, and the scheduled task remains active (Figure 5).



Figure 5 Controlware CSIRT-dnSpy

(4) They are using reverse strings or simple obfuscations (Figure 6, 7).

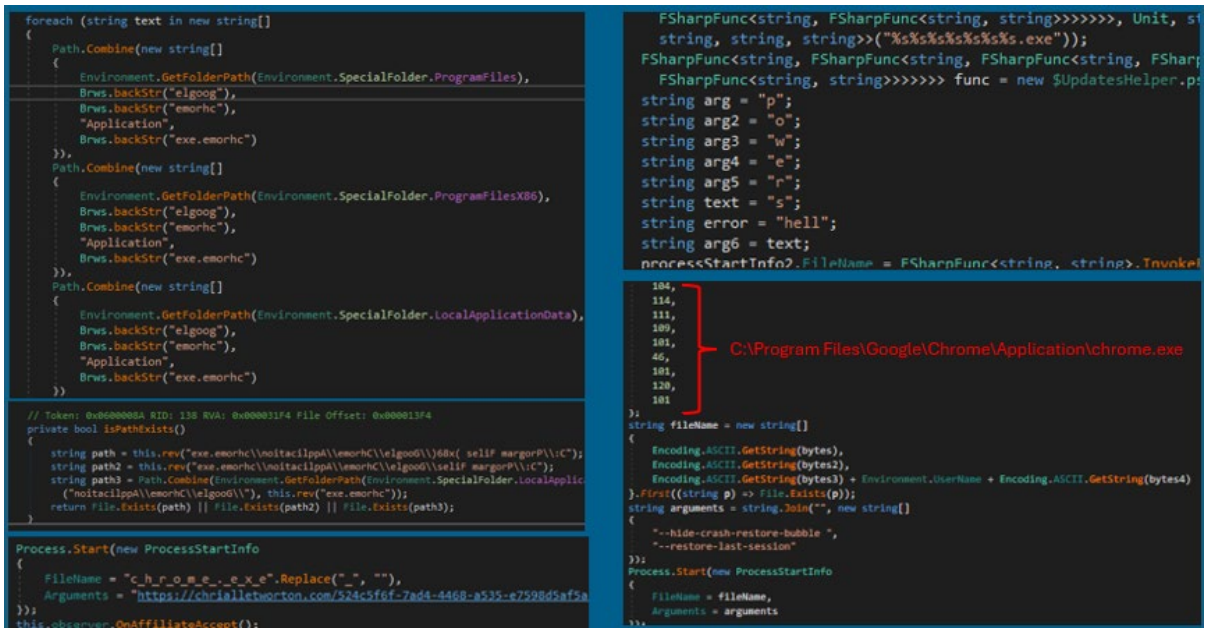


Figure 6 Controlware CSIRT-dnSpy

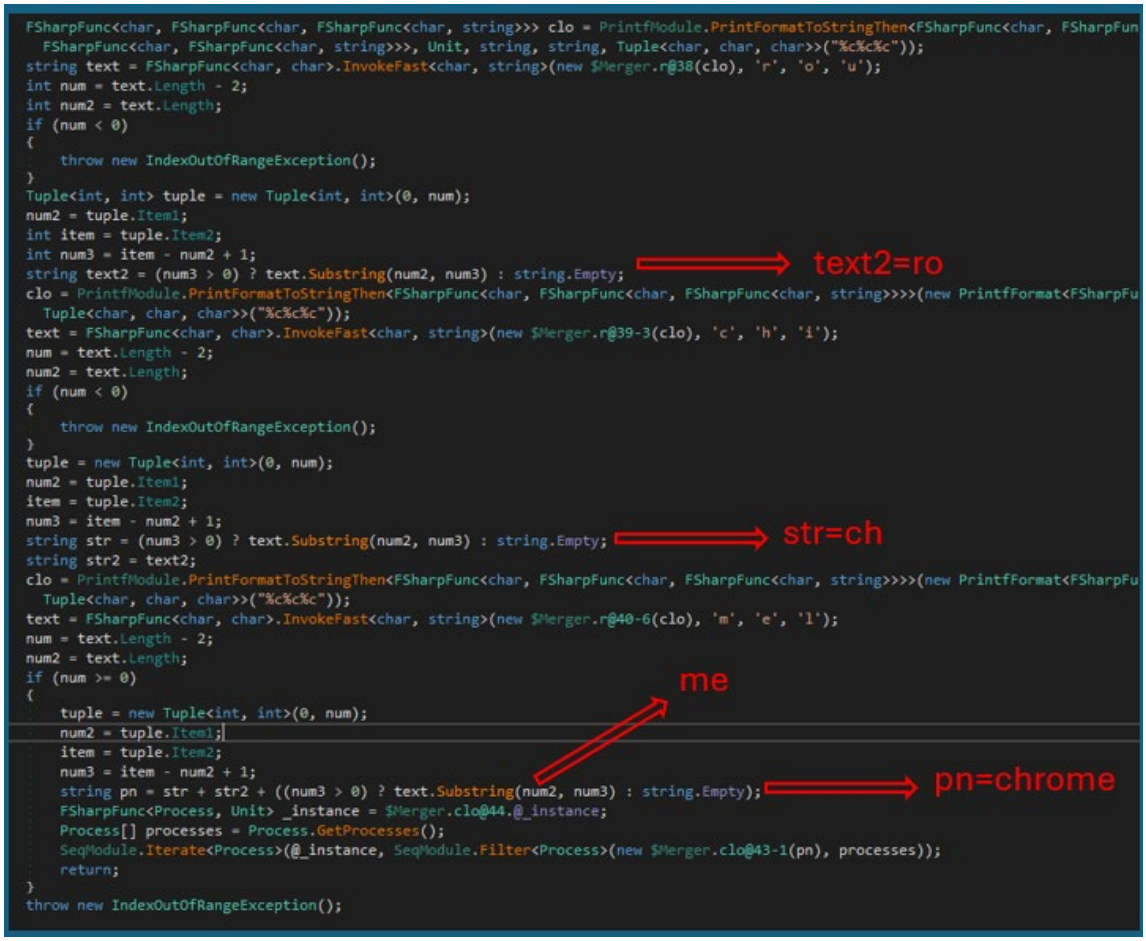


Figure 7 Controlware CSIRT-dnSpy

We identified that ConvertMate redirects users to the installation page of a Chrome extension called BriefMe (Figure 8). The extension performs its summarization function by connecting to an Amazon service, and technically it has permission to read and modify data on all visited websites. The domain listed in the extension's privacy information is not reachable, and the developer's email domain redirects to another extension download page, which belongs to a password manager. However, the extension still requires user interaction for installation, so no silent deployment is possible.

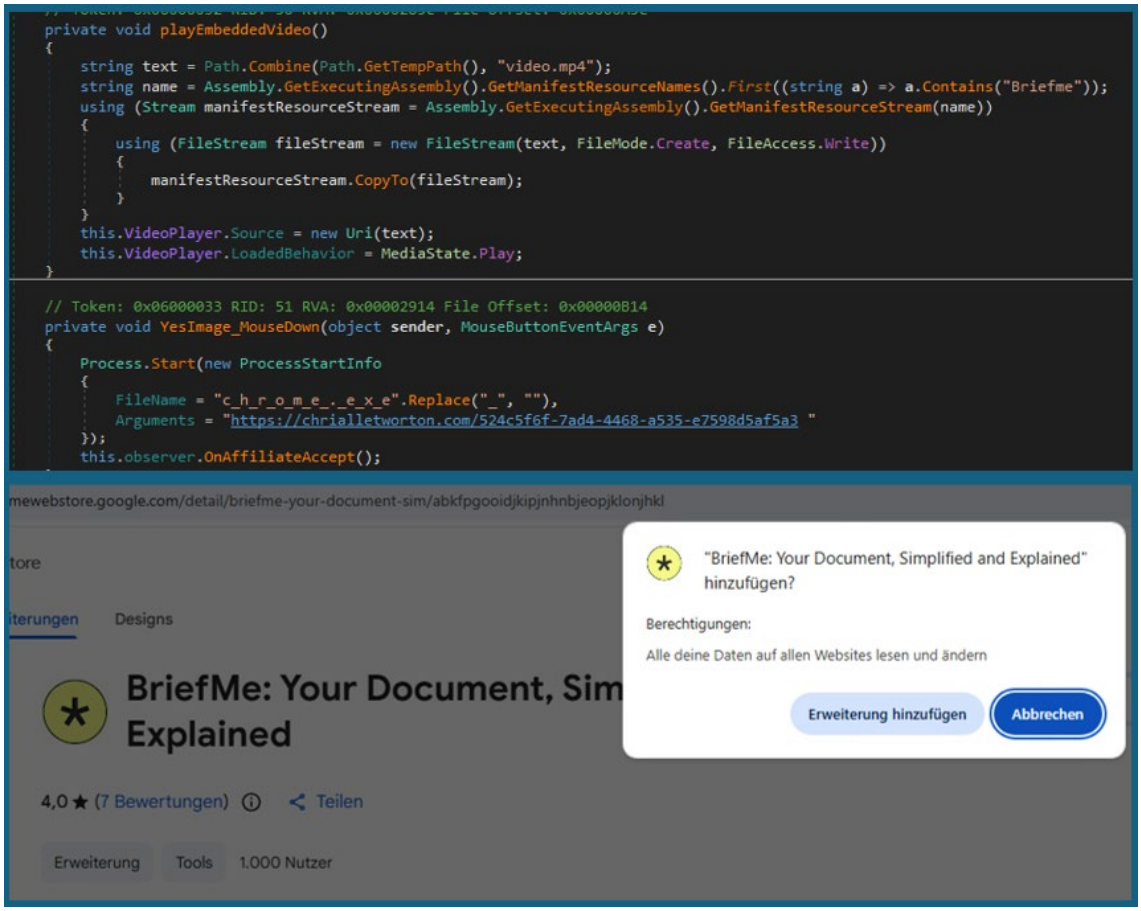


Figure 8 Controlware CSIRT-dnSpy-Chrome Web Store

(5) We detected that PowerDoc and PDFClick were performing browser hijacking (Figure 9).

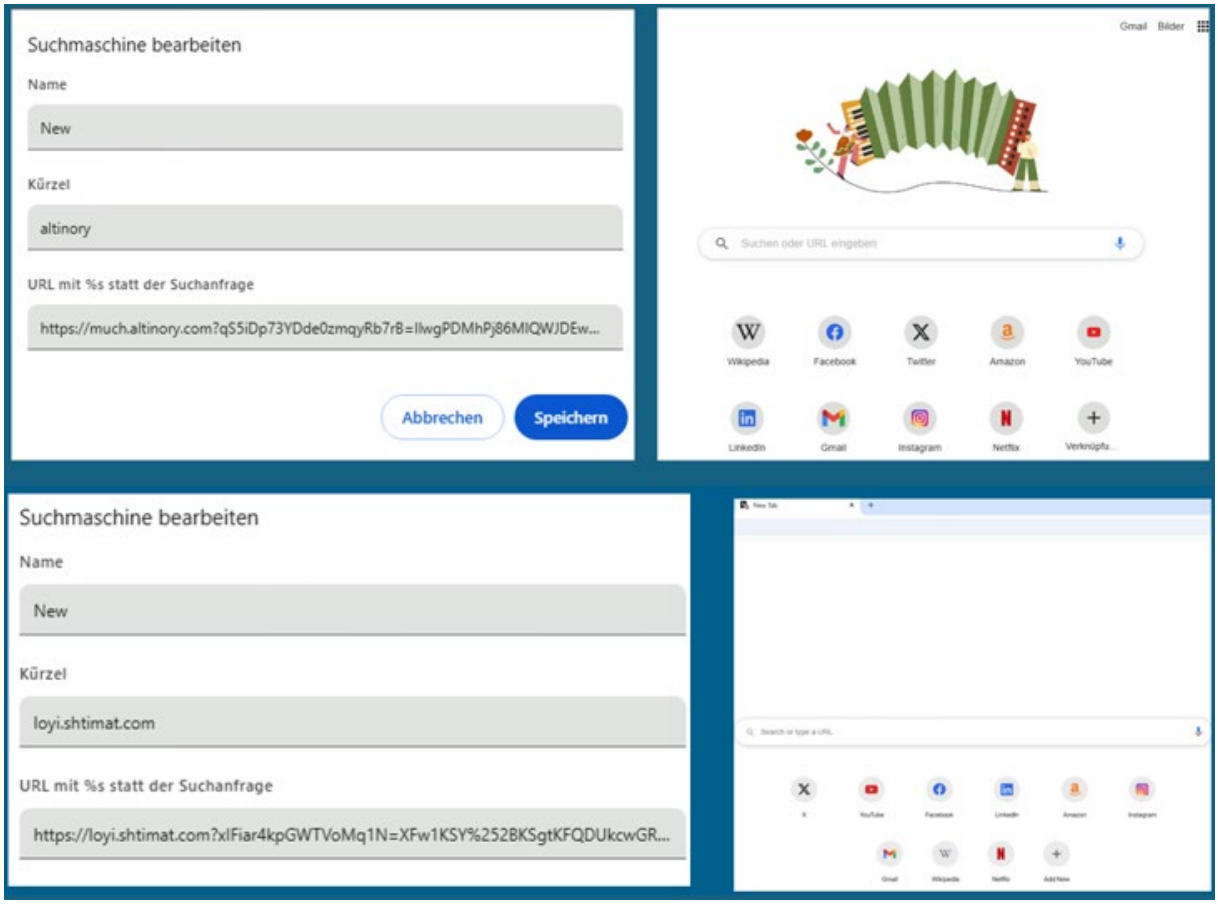


Figure 9 Controlware CSIRT-Google Chrome Browser

Threat Intelligence Findings

After analyzing the tools, we collected several indicators and used them to understand how closely these artifacts might be related. Some of the findings suggested that many of them are linked to the same ecosystem or operation. Explained below, we identified that PDFSpark differs from the other samples in several ways.

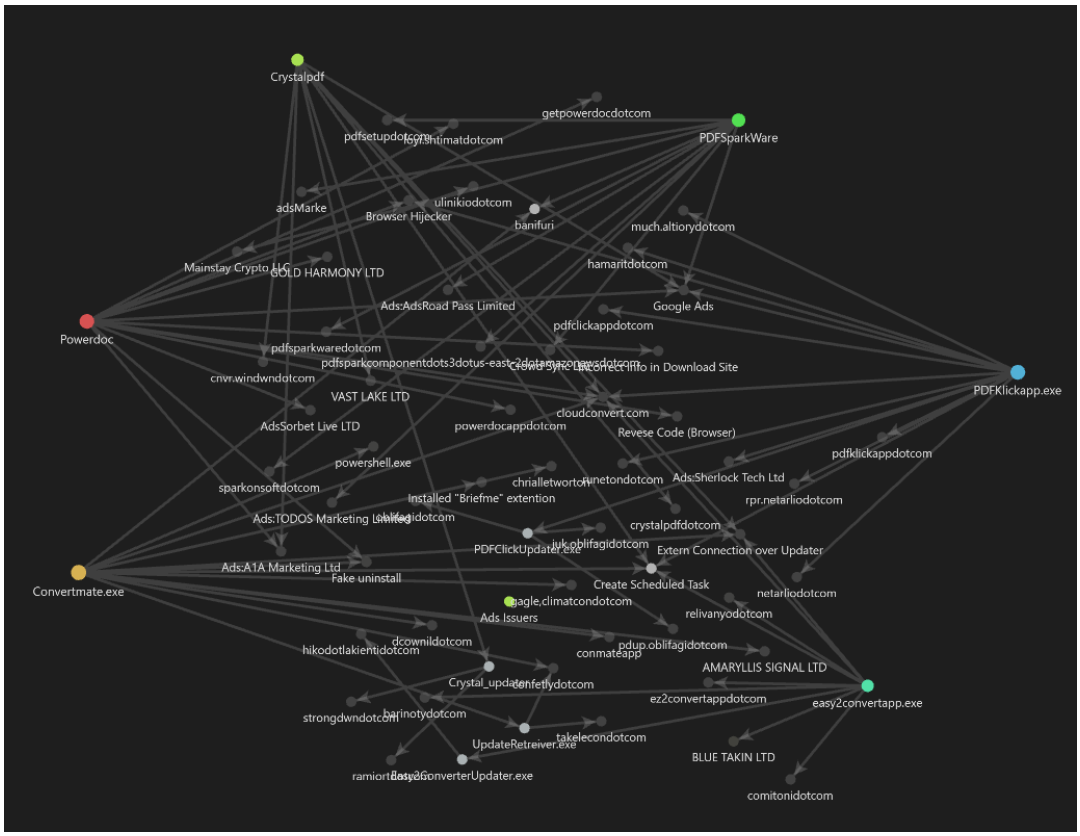


Figure 10 Obsidian Graph View

(1) Based on the domains we identified that ConvertMate and PDFSpark connect to two of the same domains (Figure11, 12). PDFSpark has two different versions, and the one signed by Crowd Sync LLC was observed to communicate with the same two domains as ConvertMate.

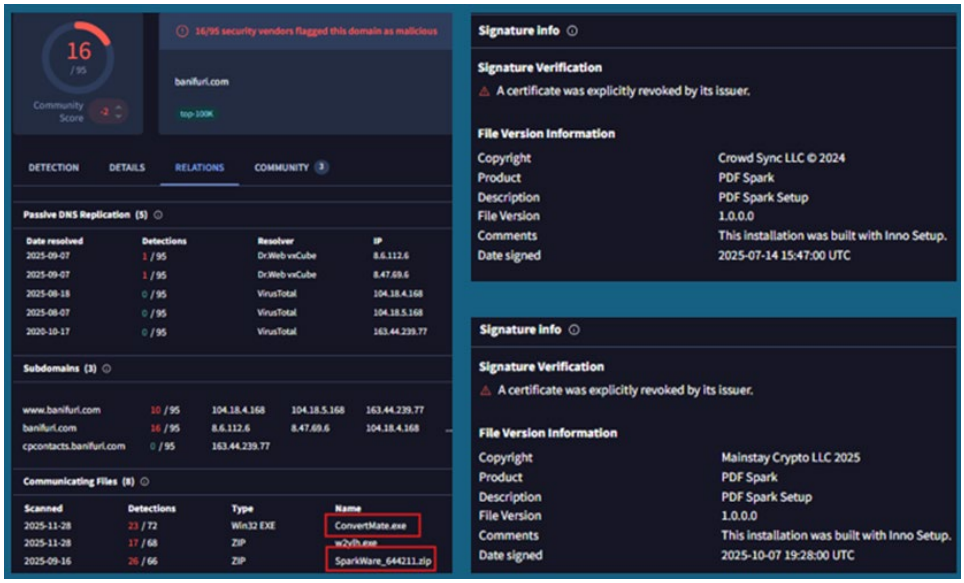


Figure 11 Virus Total

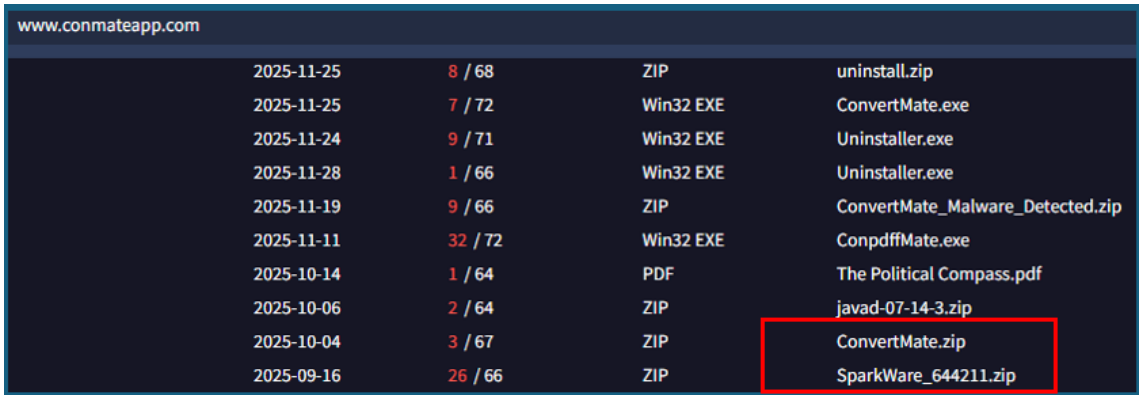


Figure 12 Virus Total

The version of PDFSpark signed by Mainstay Crypto LLC and the version signed by Crowd Sync LLC show different download mechanisms and remote communication patterns.

For example:

- The Crowd Sync LLC version downloads the converted file from pdfspark[.]s3[.]us-east-2[.]amazonaws[.]com
- The Mainstay Crypto LLC version uses different buckets: pdfsparkcomponent[.]s3[.]us-east-2[.]amazonaws[.]com, electronparts[.]s3[.]us-east-1[.]amazonaws[.]com

Additionally, PDFSpark's overall infrastructure differs from the other five tools analyzed. While the other tools are distributed as **direct .NET compiled binaries** (Easy2Convert and PDFCLick are C++, but drops a .NET updater during installation), PDFSpark is packaged using **Inno Setup**, which sets it apart from the rest.

(2) Five of the analyzed tools were found to perform PDF conversion through an external service. These tools use **CloudConvert (Figure 13),** a well-known third-party provider that offers API-based file conversion. CloudConvert is based in Germany (Lunaweb GmbH) and operates with paid, usage-based plans. This finding is notable because all the reviewed tools are distributed for free and do not display any advertisements. The fact that they spend money to provide this service without generating any revenue may indicate that the operation is motivated by other aims.

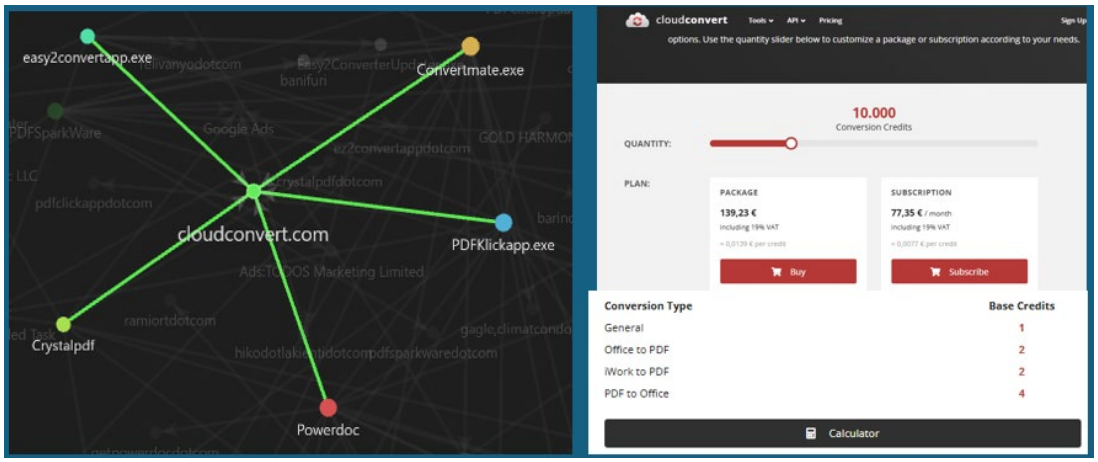


Figure 13 Obsidian-CloudConvert Official Web Page

During our analysis, we did not observe any direct CloudConvert API calls made by PDFSpark for the conversion process. Instead, the tool connects to an Amazon S3 storage service.

According to CloudConvert's documentation, converted files can be downloaded in two different ways:

(1) If there is no external export method (such as S3 or Azure), CloudConvert provides a temporary download URL (S3) valid for 24 hours.

(2) If the client has a custom export method configured, the converted file is exported directly to that storage endpoint.

These findings suggest that PDFSpark may still be using CloudConvert in the background, considering its relationship with ConvertMate, as previously noted, it would not be a surprise if this scenario were true, but it is not possible to say this for certain.

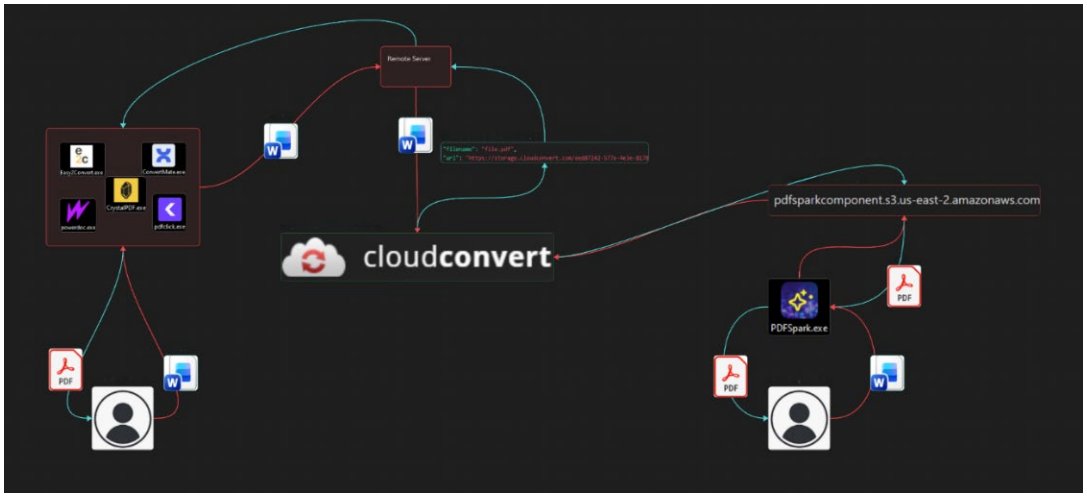


Figure 14 Controlware CSIRT-Obsidian-Canvas

(3) Domains where the tools are downloaded from and the domains, they connect to are registered through GoDaddy or Amazon and use Cloudflare as their name server. However, the situation is different in the case of PDFSpark, as the domains appear to be registered through different companies based in the Bahamas and the United States (Figure 15).

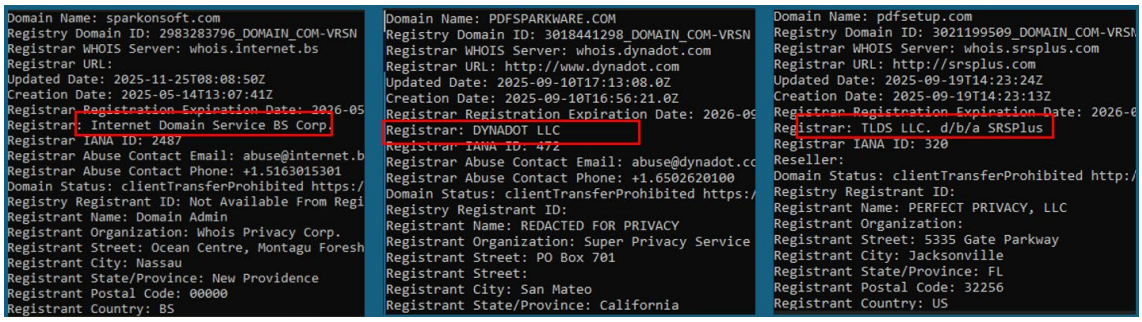


Figure 15 Controlware CSIRT-Whois Lookup

(4) The download pages contain false information (Figure 16), for example, they claim the tool works offline and does not require an internet connection.

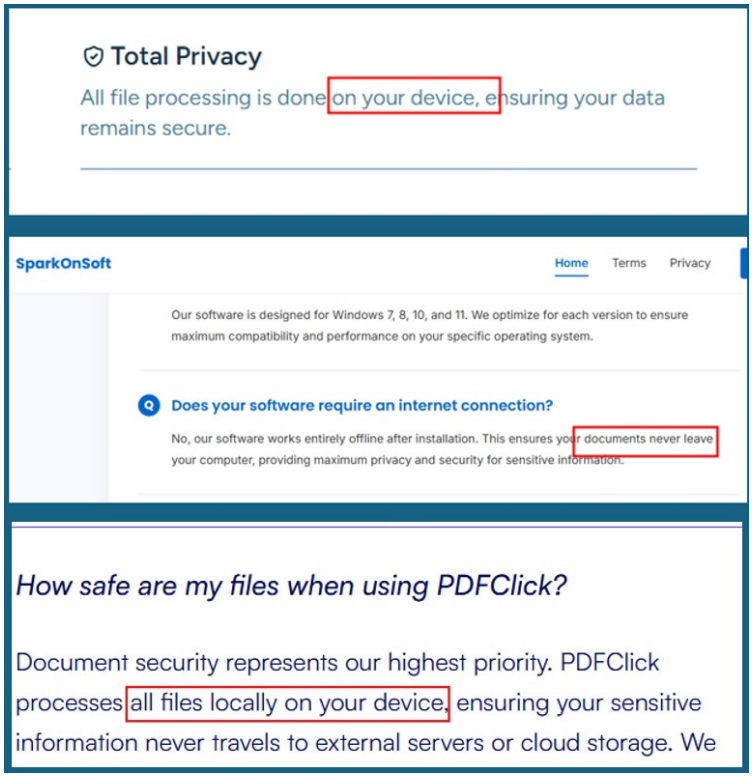


Figure 16 Controlware CSIRT-Download Pages-FAQ

(5) The download pages have a similar appearance (Figure 17), and they show similar pop-ups during the download process.

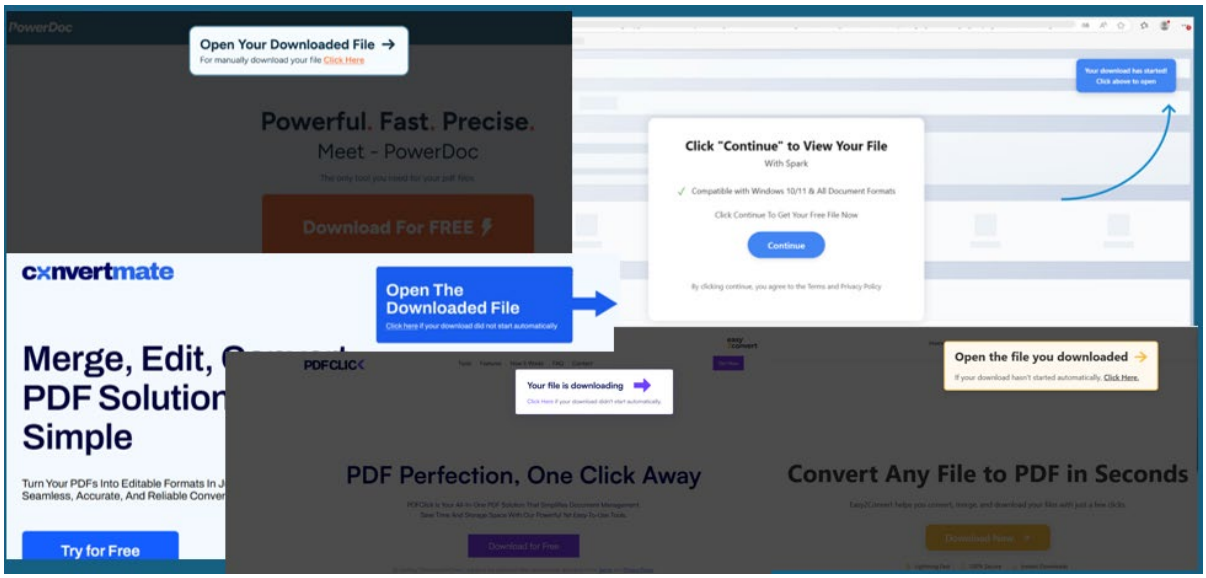


Figure 17 Controlware CSIRT-After Download

(6) Searches in the Google Ads Transparency Center show that the CrystalPDF and Powerdoc tools are distributed by the same advertiser (Figure 18). It was also observed that both are published by an additional, different advertiser.

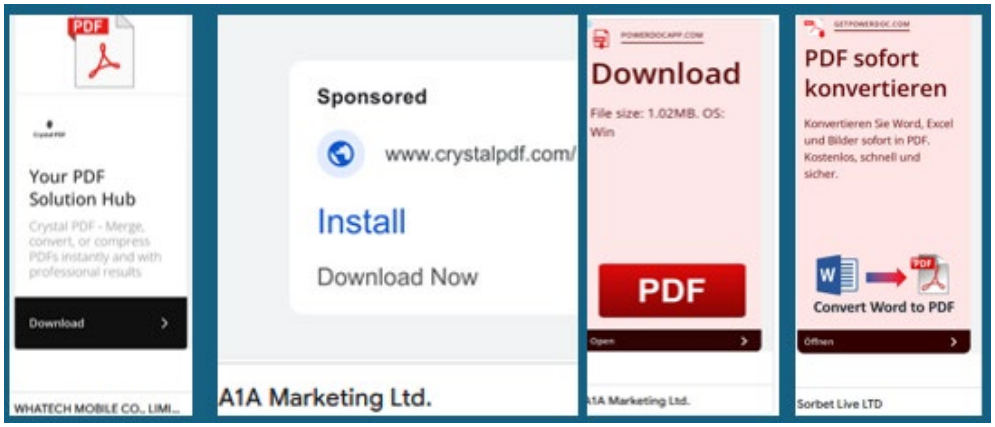


Figure 18 Google Ads Transparency Center

The download URL for CrystalPDF is no longer active; however, Powerdoc can still be downloaded from two different URLs. Since the ad campaigns remain active, we continue to detect a significant number of downloads.

(7) On the download page of ConvertMate, we identified an email address (Figure 19) in the contact section, and according to VirusTotal, the associated domain has been linked to multiple Adware/PUA samples, and even to the Neshta malware family, which is known for injecting itself into other files to spread and cause damage.

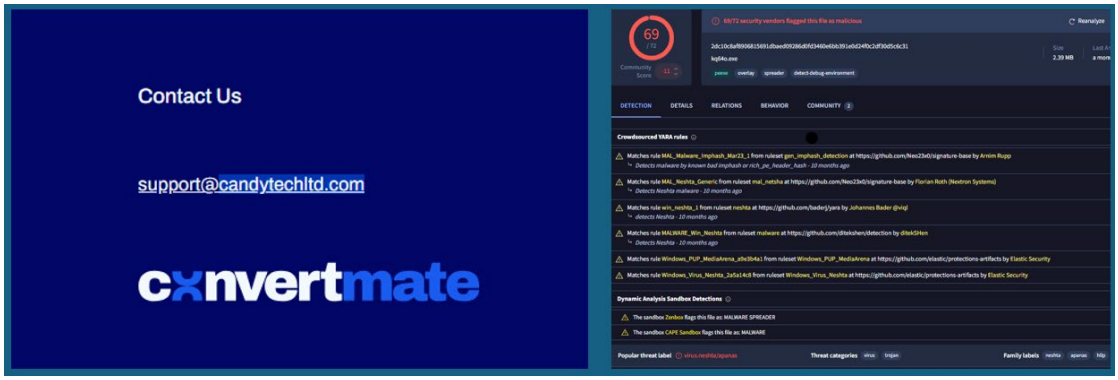


Figure 19 Download Page-Vitus Total

Many of the related files were previously signed with a code-signing certificate by the same company “CANDY TECH LTD” and were distributed under names such as “GifsMakerPro,” “ScreensRecorder,” and “ZipMakerPro.” (Figure 20).

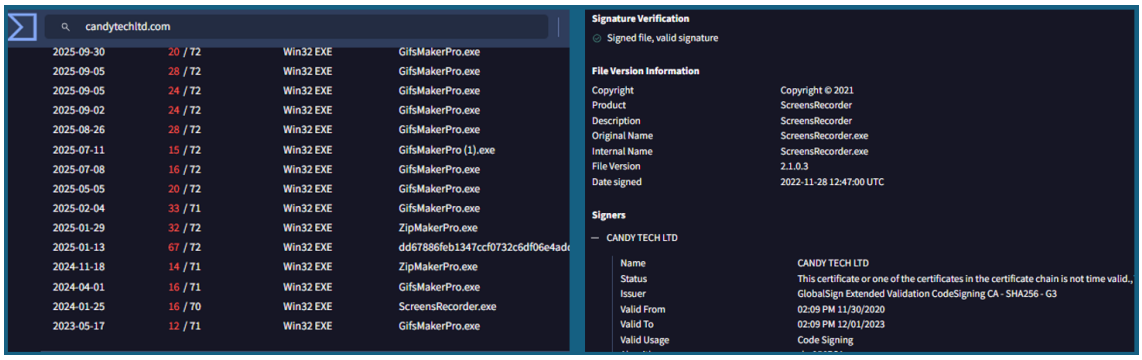


Figure 20 Virus Total

Possible Hunting Approaches

It is highly likely that the tools we analyzed represent only the visible part of the iceberg, and we can assume that many other tools with different behavior patterns are also being distributed. Therefore, focusing on detecting the dominant behaviors of the analyzed tools can at least help us identify indicators related to the known and active campaign. The hunting rules we created within this scope are provided below. False positives may occur, but the rules can be optimized over time.

To detect possible malicious PDF Tools.

```yaml
title: Executable PDF Tool Dropped in Downloads Folder by Browser
id: f77fa54d-11e5-4a25-99a6-6040329010ce
status: stable
description: Detects executable files with names containing PDF-related keywords (e.g., "pdf", "convert", "editor")
             being dropped in the Downloads folder by a web browser process. This behavior is typical of users downloading
             potentially unwanted or malicious PDF converters.
author: CSIRT Controlware
date: 2025-11-26
logsource:
  category: file_event
  product: windows
detection:
  selection:
    TargetFilename|contains:
      - '\Downloads\'
    TargetFilename|endswith: '.exe'
    TargetFilename|contains:
      - 'pdf'
      - 'convert'
      - 'editor'
    Image|endswith:
      - '\chrome.exe'
      - '\msedge.exe'
      - '\firefox.exe'
      - '\iexplore.exe'
      - '\brave.exe'
      - '\opera.exe'
  condition: selection
falsepositives:
  - Legitimate PDF converters downloaded intentionally by the user
  - Enterprise software distributed via browser
level: medium
tags:
  - attack.initial_access
  - attack.t1189
references: []
```

Figure 21 Controlware CSIRT-SIGMA rule

Some matches we found.

FileName	FileOriginUrl
pdfclick.exe	https://runeton.com/clic?fofk=e9b25a64-8496-48ca-a868-62458777bc6...
pdfclick.exe	
PDFSparkWare_225338....	
PDFSparkWare_225338....	https://pdfsparkware.com/PDFSparkWare.exe?campaign_id=230697297...
PDFSparkWare_851141....	https://pdfsparkware.com/PDFSparkWare.exe?campaign_id=230697297...

Figure 22 Controlware CSIRT-MS Defender-Advanced Threat Hunting

To detect installed potential malicious PDF Converter tools.

```yaml
title: Suspicious PDF Tool Dropping Files into AppData\Local
id: 0b6472de-c300-4fc5-864d-6d487b5354e6
status: stable
description: Detects executable files located in the Downloads folder with names related to PDF or file editing that create
             files with suspicious names (e.g., unins, update, convert) in the AppData\Local directory — a common pattern for
             malicious PDF tools.
author: CSIRT Controlware
date: 2025-11-28
logsource:
  category: file_event
  product: windows
detection:
  selection1:
    TargetFilename|contains:
      - '.txt'
      - 'unins'
      - 'update'
      - 'pdf'
      - 'convert'
      - 'edit'
    Image|contains:
      - 'pdf'
      - 'convert'
      - 'edit'
    Image|endswith: '.exe'
  selection2:
    TargetFilename|contains:
      - '\AppData\Local\'

  selection3:
    Image|contains:
      - 'Downloads'
  selection4:
    TargetFilename|contains:
      - 'Azure'
      - 'PDF24'
      - 'wps'
  condition: selection1 and selection2 and selection3 and not selection4
falsepositives:
  - Legitimate PDF editors or converters installed from Downloads
  - Custom-built applications with similar naming conventions
```

Figure 23 Controlware CSIRT- SIGMA rule

Some matches we found.

FileCreated	PDFClickUpdater.exe	C:\Users\[redacted]\AppData\Local\PDFClick\PDFClickUpdater.exe
FileCreated	Newtonsoft.Json.dll	C:\Users\[redacted]\AppData\Local\PDFClick\Newtonsoft.Json.dll
FileCreated	System.ValueTuple.dll	C:\Users\[redacted]\AppData\Local\PDFClick\System.ValueTuple.dll
FileCreated	PDFSparkWare_851141.t...	C:\Users\[redacted]\AppData\Local\Temp\is-IF2DE.tmp\PDFSparkWare_851141.tmp
FileCreated	PDFSparkWare_496571.t...	C:\Users\[redacted]\AppData\Local\Temp\is-E6RGB.tmp\PDFSparkWare_496571.tmp

Figure 24 Controlware CSIRT-MS Defender-Advanced Threat Hunting

Final Assessment

PDF converter scams demonstrate how professional attackers operate today: they combine social engineering, legitimate code-signing certificates, and technical obfuscation to remain under the radar for extended periods. This is precisely why a reactive security model is no longer sufficient.
Threat hunting is the most effective way to stay ahead of such campaigns. Only through proactive, hypothesis-driven investigation can anomalies be detected before a backdoor becomes active. Threat hunting determines time-to-detection and supports attack prevention by uncovering the preparatory steps taken by adversaries. Based on the red flags mentioned above, these tools cannot be classified as typical PUAs. The remote server communication patterns seen in the tools we analyzed indicate that they are fully capable of delivering a second-stage payload at any moment. Therefore, the most reasonable approach is to treat these tools as malware and take appropriate action.

Recommended mitigation measures

- Users should be made aware of the importance of not clicking on advertisements
- Users who really need a PDF converter should not search for it themselves on the internet and should not download it through ads
- Trusted ad blockers can be used to prevent advertisements.
- The tracking-prevention option in browsers should be enabled

IoCs

ConvertMate:
SHA256:08b9f93000512b45f8c2e8d3d6624536b366e67c40fd4b958db58e3a1d129c3d
5b4861baeb563875c99614bd6586a9e3b1bd2fef835afffa03210e86eeb6c775
dcownil[.]com
conmateapp[.]com
banifuri[.]com
takelecon[.]com
chrialletworton[.]com
confetly[.]com
climatcon[.]com

CrystalPDF:
SHA256:0602811ee5babfd67089b9adb3397201924fc86943a1a544c3d6dd66a18fc16c
51d4b6935205b8aef162daa87935ee0f0fb6a1b3fedcaaadff2eaa8075aaf3fe
crystalpdf[.]com
ramiort[.]com
strongdwn[.]com
windwn[.]com
negmari[.]com

Easy2Convert:
SHA256:c60a9792f93e923834545153ec31f3420878c0d94c011a6b7ef30b5a2074a38a
27262f4bf8096f04e53309d4ce603cfbeb27ed10abdf1c461d3ccb14e012f61e
ez2convertapp[.]com
comitoni[.]com
barinoty[.]com
relivanyo[.]com
hagalilk[.]com
eloknys[.]com

PDF Spark:
SHA256:415b6d1bb78cb74a468b29e7af09e885999cfcabf2c413f3bf533c2191d4e626
7ed76946c8ef0829f1011ce230cae7b63c3bf061de1e5f9d8da616a97ad6e4c5
pdfsparkware[.]com
sparkonsoft[.]com
pdfsetup[.]com
pdfsparkapi[.]com

PowerDoc:
SHA256:b3afc517095d0362a32c5655f7572123e5db2e09fe24f6f917b880d6a969c682
ulinikio[.]com
getpowerdoc[.]com
shtimat[.]com
powerdocapp[.]com

PdfClick:
SHA256:09474277051fc387a9b43f7f08a9bf4f6817c24768719b21f9f7163d9c5c8f74
50651ed57b60d48da11117a170241da8669bf0e6e7ea76d7f2d364db80e16d6f
pdfclickapp[.]com
runeton[.]com
hamarit[.]com
netarlio[.]com
altinory[.]com
oblifagi[.]com

At the beginning of April, we identified a **StealC Stealer** distribution campaign through **printables.com**, a legitimate 3D model-sharing platform.

Appendix A Locations

Locations in Germany

Company Headquarters
Controlware GmbH
Waldstraße 92
63128 Dietzenbach

Tel: +49 6074 858-00
Fax: +49 6074 858-108
E-Mail: info(at)controlware.de

Berlin
Controlware GmbH
Justus-von-Liebig-Straße 7
12489 Berlin

Tel.: +49 30 67097-0
Fax: +49 30 67097-111
E-Mail: info-ber(at)controlware.de

Dortmund
Controlware GmbH
Adi-Preißler-Allee 4
44309 Dortmund

Tel.: +49 231 229685-00
Fax: +49 231 229687-99
E-Mail: info-dtm(at)controlware.de

Düsseldorf
Controlware GmbH
Meerbuscher Straße 78
40670 Meerbusch

Tel.: +49 2159 9696-0
Fax: +49 2159 9696-96
E-Mail: info-due(at)controlware.de

Hamburg
Controlware GmbH
Am Stadtrand 56
22047 Hamburg

Tel.: +49 40 251746-0
Fax: +49 40 251746-46
E-Mail: info-ham(at)controlware.de

Brandboxx Hanover
Controlware GmbH / B125
Hessenstraße 1
30855 Langenhagen

Tel.: +49 511 726092-0
Fax: +49 511 726092-20
E-Mail: info-han(at)controlware.de

Ingolstadt
Controlware GmbH
Marie-Curie-Str. 22
85055 Ingolstadt

Tel.: +49 841 23222-0
Fax: +49 841 23222-208
E-Mail: info-ing(at)controlware.de

Kassel
Controlware GmbH
Heinrich-Hertz-Straße 3b
34123 Kassel

Tel: +49 561 47576-0
Fax: +49 561 47576-29
E-Mail: info-kas(at)controlware.de

Leipzig
Controlware GmbH
Eilenburger Straße 1a
04317 Leipzig

Tel.: +49 341 98387-30
Fax: +49 341 98387-33
E-Mail: info-lei(at)controlware.de

Munich
Controlware GmbH
Inselkammerstraße 1
82008 Unterhaching

Tel.: +49 89 666367-0
Fax: +49 89 666367-77
E-Mail: info-muc(at)controlware.de

Stuttgart
Controlware GmbH
Raiffeisenstraße 16
70794 Filderstadt

Tel.: +49 711 770568-0
Fax: +49 711 770568-150
E-Mail: info-stu(at)controlware.de

Wolfsburg
Controlware GmbH
Wolfsburger Straße 13
38554 Weyhausen

Tel.: +49 5362 9993413
Fax: +49 511 726092-20
E-Mail: info-wey(at)controlware.de

Locations in Austria

Innsbruck
Controlware GmbH
Grabenweg 68
Soho 2, 2. Stock
A-6020 Innsbruck
Österreich

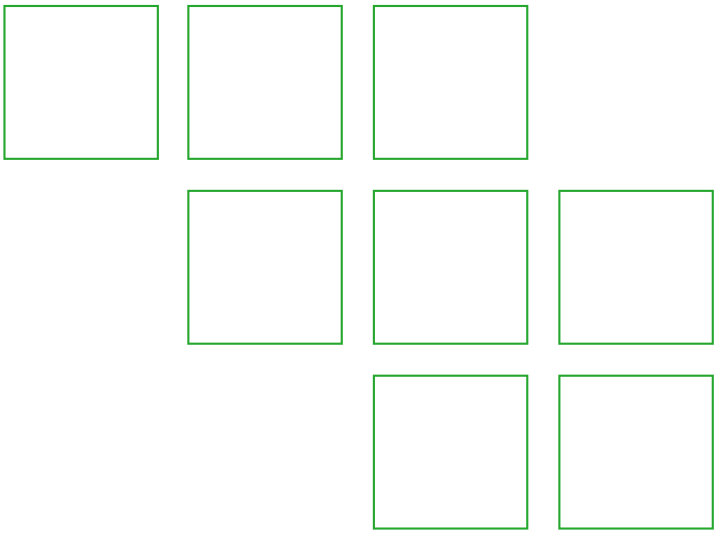
Tel.: +43 512 345200
Fax: +43 512 3452006015
E-Mail: info(at)controlware.at

Vienna
Controlware GmbH
Handelskai 92
Rivergate C1 / 4.OG / Top F01
A-1200 Wien
Österreich

Tel.: +43 1 890 0724-0
E-Mail: info(at)controlware.at

Ihre IT.
Heute. Für morgen.

controlware



Controlware GmbH, Waldstraße 92, 63128 Dietzenbach, Germany
T +49 6074 858-00, F +49 6074 858-108, info@controlware.de, www.controlware.de
Registergericht Offenbach a.M., HRB Nr. 6431, USt-IdNr. DE 113 539 225, Steuernummer 04423035231
Geschäftsführer: Bernd Schwefing, Michael Küchen, Aufsichtsratsvorsitzender: Christof Ziegler