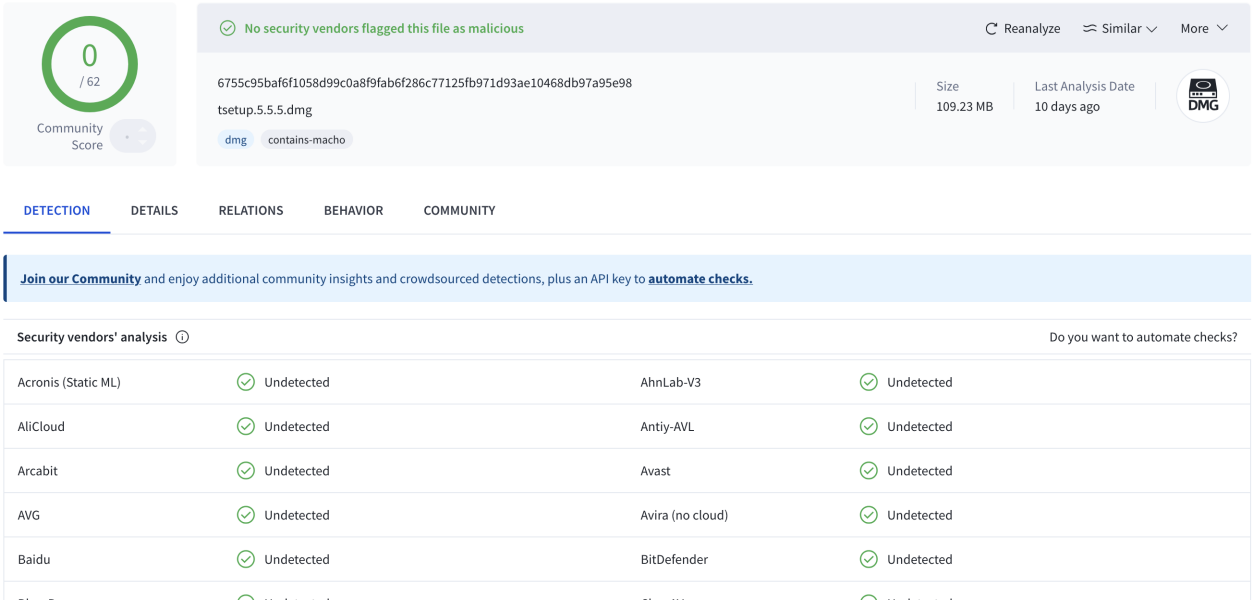
Relazione Malware Analysis

Di seguito viene fornita una breve relazione sullo studio effettuato degli strumenti per l'analisi dei malware visti a lezione

VirusTotal

Il file utilizzato per l’analisi di **VirusTotal** è il setup di Telegram Desktop per macOS



Ad una prima ispezione, il file testato non presenta nessun indicatore che suggerisca intenti malevoli del file

Basic properties

MD5	49012608bfc8cf889b381f734859bbed
SHA-1	d4c7fc5ca9b25502aaac994ea1aab192e69c4d96
SHA-256	6755c95baf6f1058d99c0a8f9fab6f286c77125fb971d93ae10468db97a95e98
Vhash	ec8c983666ed1948c8550927e86713ff
SSDEEP	3145728:kJg/QXlpSu7vZHkjvUdi/WTVrxWg4VXb1mw5BXzH8BXe00G5y:Igslp5vVQ/AbUX5RpcBsEy
TLSH	T17A48337E29C16C92F5C945F05C821535DE590E533A46D8F2D2ABFE31203BEB97A38319
File type	Macintosh Disk Image executable mac dmg
Magic	DOS/MBR boot sector, extended partition table (last) (bzip2 compressed data, block size = 100k)
TrID	Macintosh Disk image (BZ2 compressed) (96.3%) | bzip2 compressed archive (3.6%)
Magika	DMG
File size	109.23 MB (114539906 bytes)

History

First Submission	2024-09-13 20:37:34 UTC
Last Submission	2024-09-23 14:13:25 UTC
Last Analysis	2024-09-13 20:37:34 UTC

Names

tsetup.5.5.5.dmg

telegram-for-desktop-5-5-5.dmg

Approfondendo l'analisi, VirusTotal le firme **MD5, SHA-1, SHA-256** del file. Questi hash servono a verificare l’integrità e l’autenticità del file, permettendo di confrontarli con database di malware noti.

VirusTotal ci mostra poi che il file è un’immagine disco di Macintosh (Macintosh Disk Image) di dimensione 109.23 MB. Questa dimensione è coerente con le aspettative rispetto a questo tipo di file. Un indicatore anomalo ci avrebbe invece suggerito che del codice malevolo potrebbe essere nascosto all'interno dell'eseguibile (e.g. trojan)

VirusTotal segnala che il file è stato identificato come **tsetup.5.5.5.dmg** e **telegram-for-desktop-5-5-5.dmg**, indicando che si tratta realmente del setup di Telegram Desktop.

File System Property List

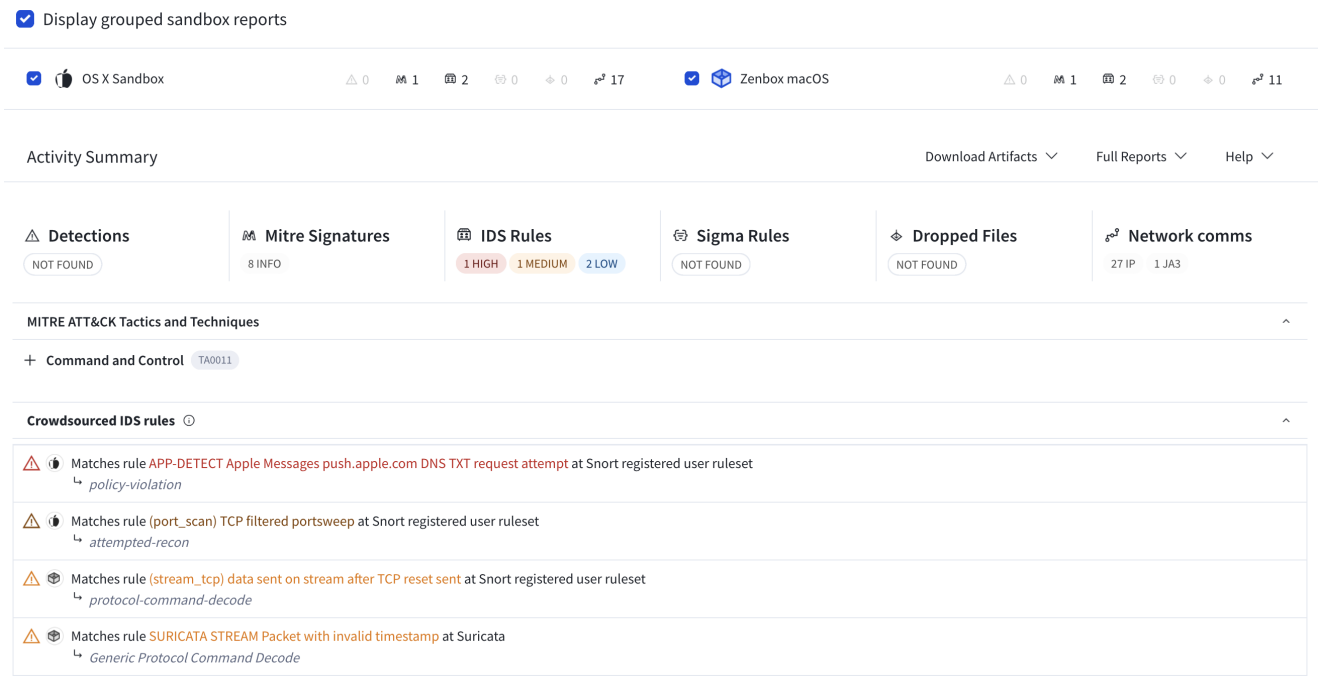
CFBundleInfoDictionaryVersion	6.0
DTXcodeBuild	15F31d
CFBundleGetInfoString	Telegram Desktop messaging app
CFBundleIdentifier	com.tdesktop.Telegram
DTSDKName	macosx14.5
DTPlatformVersion	14.5
NSMicrophoneUsageDescription	We need access to your microphone so that you can record voice messages and make calls.
CFBundleShortVersionString	5.5.5
NSCameraUsageDescription	We need access to your camera so that you can record video messages and make video calls.
LSFileQuarantineEnabled	True
BuildMachineOSBuild	23G93
CFBundleExecutable	Telegram
LSMinimumSystemVersion	10.13
CFBundleVersion	5.5.5
CFBundleIconFile	AppIcon
NSLocationUsageDescription	We need access to your location so that you can send your current locations.
DTXcode	1540
CFBundleURLTypes	[{'CFBundleTypeRole': 'Viewer', 'CFBundleURLIconFile': 'Icon.icns', 'CFBundleURLName': 'com.tdesktop.Telegram', 'CFBundleURLSchemes': ['tg', 'tonsite']}]
DTPlatformName	macosx
CFBundleIconName	AppIcon
LSApplicationCategoryType	public.app-category.social-networking
CFBundleSupportedPlatforms	['MacOSX']
DTCompiler	com.apple.compilers.llvm.clang.1_0
CFBundleSignature	????
NSSupportsAutomaticGraphicsSwitching…	True
DTSDKBuild	23F73
CFBundleName	Telegram
ITSAppUsesNonExemptEncryption	False
CFBundlePackageType	APPL
NSPrincipalClass	NSApplication

In questo caso, oltre a verificare informazioni come il **CFBundleIdentifier**, il **CFBundleExecutable** e il **CFBundleGetInfoString**, che sembrano confermare la legittimità dell'eseguibile, notiamo che l'applicativo richiede l'accesso al microfono, alla camera del pc e alla nostra posizione. Tuttavia, come spiegato nei rispettivi campi (**NSMicrophoneUsageDescription**, **NSCameraUsageDescription** e **NSLocationUsageDescription**), l'utilizzo di questi servizi sembra legittimo e coerente con il funzionamento dell'applicazione

Contacted IP addresses (27)

IP	Detections	Autonomous System	Country
17.145.48.1	0 / 94	714	US
17.179.252.2	0 / 94	714	US
17.188.143.125	0 / 94	714	US
17.188.143.157	0 / 94	714	US
17.188.143.158	0 / 94	714	US
17.188.143.187	0 / 94	714	US
17.188.178.226	0 / 94	714	US
17.188.178.34	0 / 94	714	US
17.188.179.2	0 / 94	714	US
17.188.179.34	0 / 94	714	US

Questa schermata mostra invece un elenco di indirizzi IP con i quali il processo avviato dal file ha stabilito una connessione. Notiamo che tutti gli indirizzi provengono dagli Stati Uniti e che nessuno indicato come sospetto o malevolo.



Per concludere, il rapporto di VirusTotal, basato su un'analisi comportamentale in ambienti sandbox (OS X Sandbox e Zenbox macOS), non rileva minacce dirette.

Tuttavia, viene segnalato un comportamento potenzialmente rischioso: una richiesta DNS a un server di Apple (apple.com) per un record TXT, indicata come possibile violazione della privacy (`privacy-violation`). In realtà, questa richiesta è plausibile e dimostra che Apple verifica l'autenticità dell'applicazione. Il file ha anche eseguito una scansione delle porte aperte (`port-scan`) e stabilito una comunicazione TCP (`stream-tcp`), che potrebbe

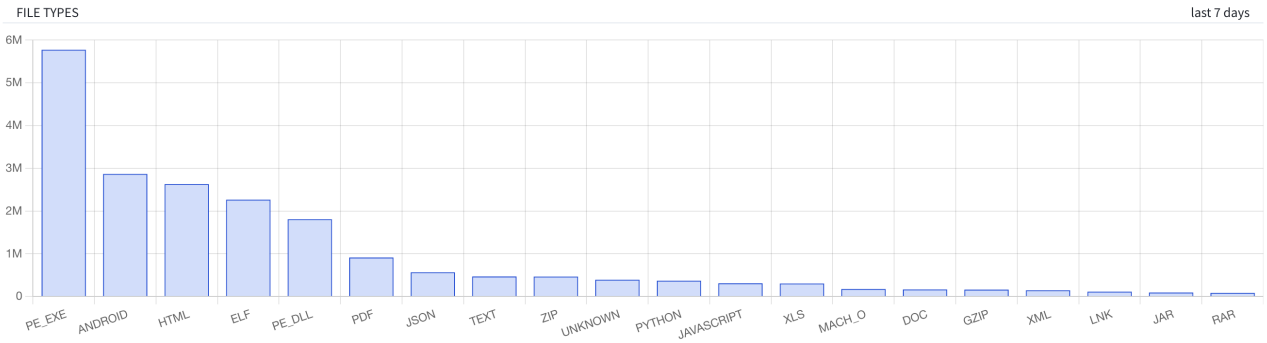
sembrare sospetta, ma è coerente con la richiesta DNS fatta ai server Apple (abbiamo inoltre già appurato che gli indirizzi IP utilizzati sono legittimi)

AnyRun

Per quanto riguarda **AnyRun**, a causa dei limiti della piattaforma (la versione gratuita accetta infatti file di dimensione $\leq$ 16 MB) e al fatto che non è possibile emulare il sistema operativo macOS, è stato testato un file PDF anziché il file dmg

---

La legittimità di questo tipo di analisi è garantita da VirusTotal, che ci mostra come i pdf siano tra i file non eseguibili più pericolosi



source: https://www.virustotal.com/gui/stats

Le informazioni preliminari fornite da AnyRun confermano che il file è effettivamente un PDF, con firme digitali generate utilizzando diverse tecniche di hashing (MD5, SHA1 e SHA256). Ancora una volta, questi hash possono essere impiegati per valutare la potenziale pericolosità del file.

General Info

Add for printing

File name:	flex__bison.pdf
Full analysis:	https://app.any.run/tasks/209c2950-057f-41ae-802f-2b5c162fc646
Verdict:	No threats detected
Analysis date:	September 25, 2024 at 15:28:47
OS:	Windows 10 Professional (build: 19045, 64 bit)
Tags:	qrcode
Indicators:	
MIME:	application/pdf
File info:	PDF document, version 1.4
MD5:	F9DE480E4028D88B35D3F29A4168A933
SHA1:	08795332BB60A74BF17D65E4895AACF9B69DB317
SHA256:	BC4660090AEA25E28E58F5CCDC717E7464DC0A97CAFC9B8A7CB9698B194FAC18
SSDEEP:	98304:xgnFx3PPDTaSaZaq9SOLHvAk5ufAp8sexoBgT0AHstJcibv72PemZGgX+AJrYW7Y:Enr8V

In questo caso, AnyRun non ha rilevato alcuna minaccia associata al file (`no threats detected`)

TRiD

.arff | Attribute-Relation File Format (with rem) (69.6)
.pdf | Adobe Portable Document Format (30.3)

EXIF

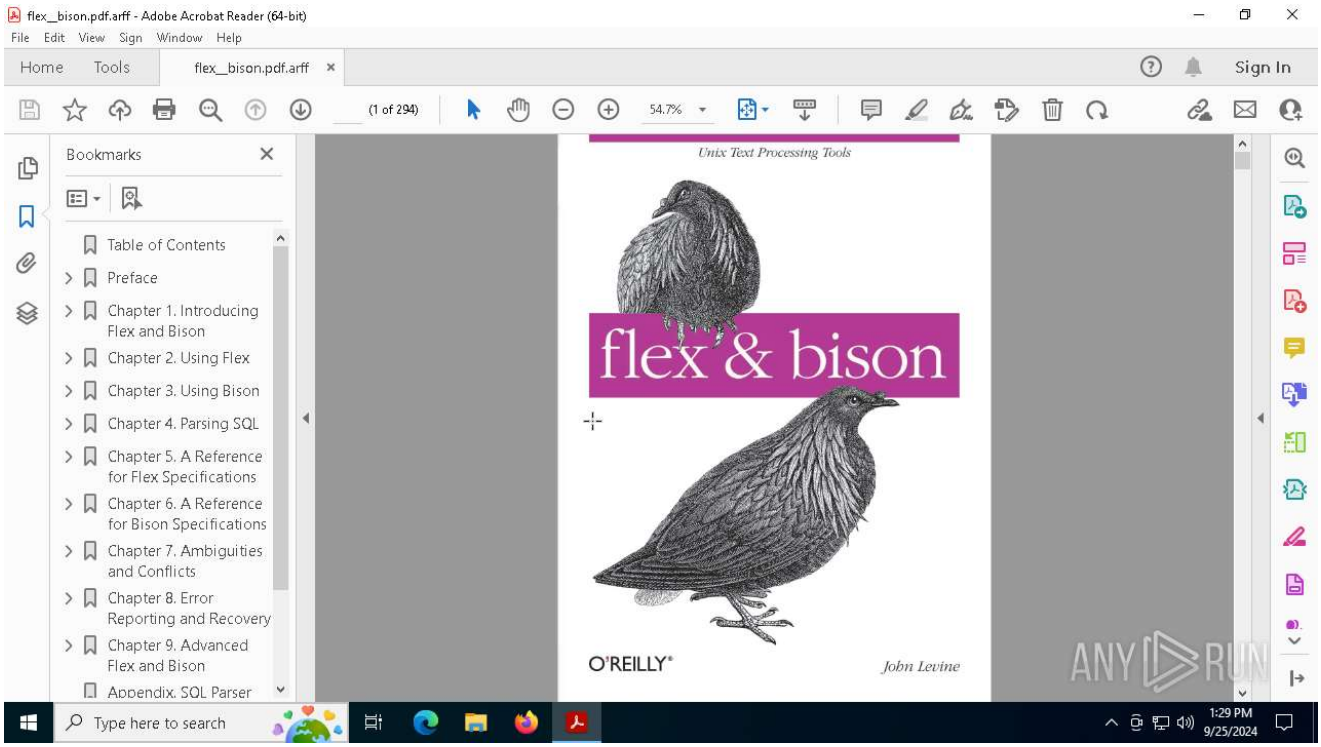
PDF

PDFVersion:	1.4
Linearized:	No
HasXFA:	No
PageLayout:	SinglePage
PageMode:	UseOutlines
PageCount:	294
Author:	John R. Levine
CreateDate:	2009:08:04 13:18:05-05:00
Creator:	XSL Formatter V4.3 R1 (4,3,2008,0424) for Linux
ModifyDate:	2012:09:25 15:36:05+05:30
Producer:	Antenna House PDF Output Library 2.6.0 (Linux)
Title:	flex & bison
Trapped:	-

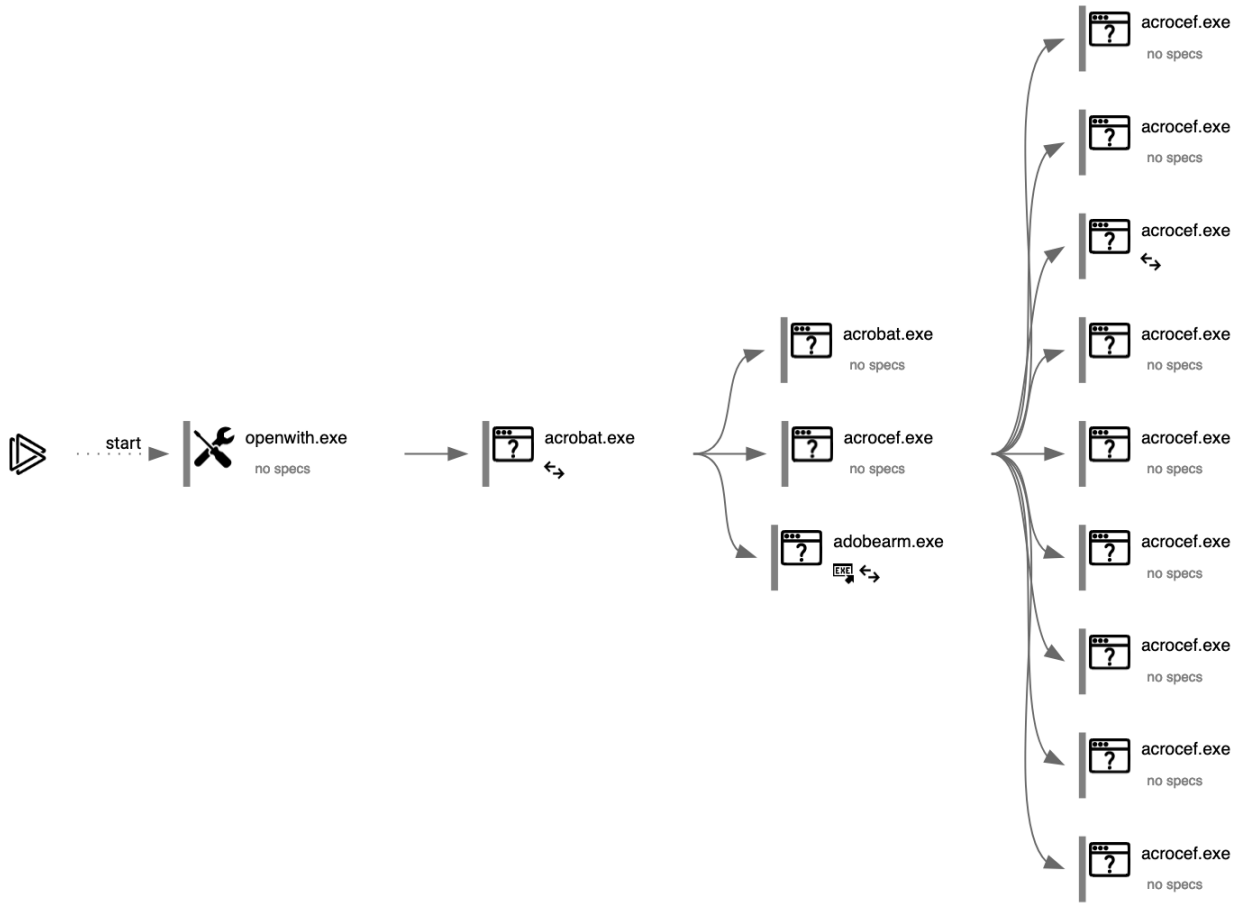
XMP

XMPToolkit:	Adobe XMP Core 4.2.1-c041 52.342996, 2008/05/07-20:48:00
CreateDate:	2009:08:04 13:18:05-05:00
CreatorTool:	XSL Formatter V4.3 R1 (4,3,2008,0424) for Linux
ModifyDate:	2009:08:27 14:27+07:00
MetadataDate:	2009:08:27 14:27+07:00
Format:	application/pdf
Creator:	John R. Levine
Title:	flex & bison
Producer:	Antenna House PDF Output Library 2.6.0 (Linux)
Trapped:	-
DocumentID:	uuid:d010e595-5e99-4dc2-81b5-b78cb04aa848
InstanceID:	uuid:982612d4-5bf9-4c44-a0cd-9a21a38ec46c

Attraverso un'analisi statica preliminare, AnyRun ha fornito diverse informazioni sul documento sottoposto. In questo caso, i dati relativi all'**autore**, al **produttore**, alla **data di creazione** e al **numero di pagine** risultano coerenti con quelli reperibili online



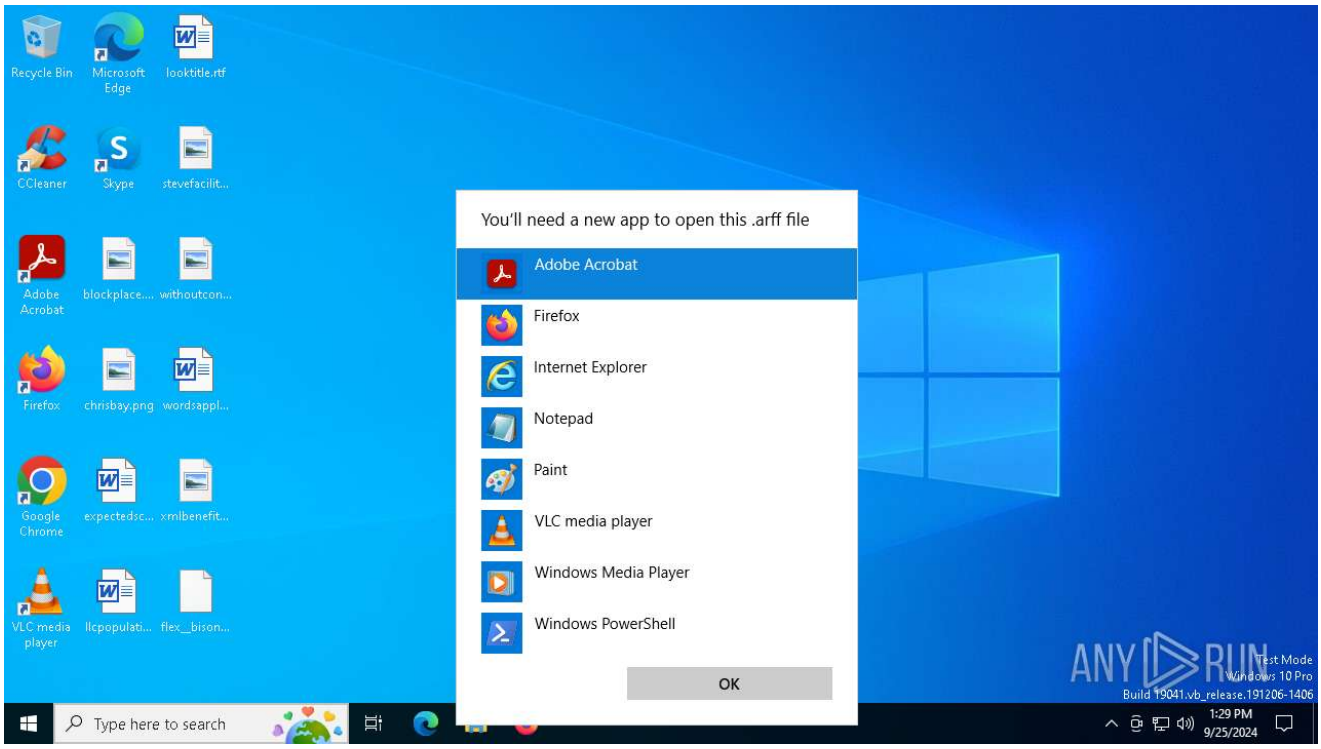
Utilizzando l’interfaccia di AnyRun, sono stato in grado di esaminare il contenuto del PDF sottoposto



Process information

PID	CMD	Path	Indicators	Parent process
1116	"C:\WINDOWS\System32\OpenWith.exe" C:\Users\admin\Desktop\flex__bison.pdf.arff	C:\Windows\System32\OpenWith.exe	–	explorer.exe
	Information			
4472	"C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe" "C:\Users\admin\Desktop\flex__bison.pdf.arff"	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe	⇄	OpenWith.exe
	Information			
5208	"C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe" --type=renderer /prefetch:1 "C:\Users\admin\Desktop\flex__bison.pdf.arff"	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe	–	Acrobat.exe
	Information			
6392	"C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\AcroCEF.exe" --backgroundcolor=16514043	C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\AcroCEF.exe	–	Acrobat.exe
	Information			

L’analisi dei processi avviati durante il test mi ha permesso di identificare due eseguibili: *OpenWith.exe* (il programma che consente di scegliere quale applicazione utilizzare per aprire il file, come mostrato di seguito) e *Acrobat.exe* (il visualizzatore di file PDF, mostrato in precedenza)



Non sono quindi stati lanciati in background processi potenzialmente malevoli

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
14	37	19	0

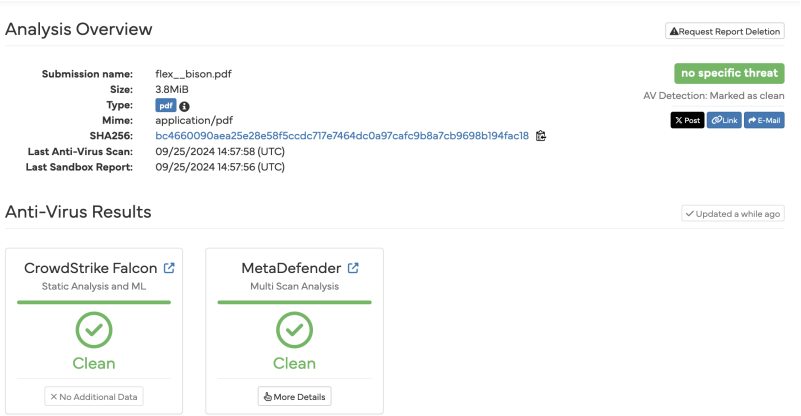
Per concludere, analizziamo il traffico di rete generato durante l'avvio del programma. In totale, sono state effettuate 14 richieste HTTP, 37 connessioni TCP/UDP e 19 richieste a server DNS, principalmente originate da *Acrobat.exe*

Domain	IP	Reputation
settings-win.data.microsoft.com	20.73.194.208 4.231.128.59	whitelisted
www.microsoft.com	184.30.21.171	whitelisted
google.com	142.250.185.206	whitelisted
login.live.com	40.126.32.138 40.126.32.76 40.126.32.140 20.190.160.20 40.126.32.133 40.126.32.74 40.126.32.136 40.126.32.68	whitelisted
ocsp.digicert.com	192.229.221.95	whitelisted
geo2.adobe.com	23.218.208.137	whitelisted
p13n.adobe.io	52.5.13.197 52.202.204.11 23.22.254.206 54.227.187.23	whitelisted
acroipm2.adobe.com	23.48.23.51 23.48.23.54	whitelisted
armmf.adobe.com	184.30.20.134	whitelisted
slscr.update.microsoft.com	52.165.165.26	whitelisted
fe3cr.delivery.mp.microsoft.com	13.95.31.18	whitelisted
ardownload3.adobe.com	23.48.23.25 23.48.23.39	whitelisted
nexusrules.officeapps.live.com	52.111.229.48	whitelisted

I server contattati appartengono però ad aziende note: Adobe (adobe.com) e Microsoft (microsoft.com e live.com). Inoltre, nessuno degli indirizzi IP utilizzati nelle connessioni risulta sospetto, in quanto sono presenti nelle "liste di fiducia" (`whitelisted`). Possiamo quindi confermare che il file non contiene alcun tipo di malware.

Hybrid Analysis

Ho infine sottoposto lo stesso file PDF a Hybrid Analysis per effettuare un confronto tra le due piattaforme



Anche questa volta non sono emerse criticità nel file. Approfondendo l'analisi, anche l'ambiente sandbox **Falcon** di Hybrid Analysis fornisce alcune informazioni di base, come la

firma del file e il nome del **produttore**

flex__bison.pdf

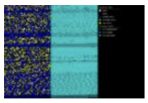
Filename	flex__bison.pdf
Size	3.8MiB (3996302 bytes)
Type	pdf
Description	PDF document, version 1.4
Document creator	XSL Formatter V4.3 R1 (4,3,2008,0424) for Linux
Document producer	Antenna House PDF Output Library 2.6.0 (Linux)
Document title	flex & bison
Document pages	294
Architecture	WINDOWS
SHA256	bc4660090aea25e28e58f5ccdc717e7464dc0a97cafc9b8a7cb9698b194fac18
MD5	f9de480e4028d88b35d3f29a4168a933
SHA1	08795332bb60a74bf17d65e4895aacf9b69db317
ssdeep	49152:YGMVib07KmGBUlouyAC5Pa7cQFpDYqXbC9OaE+7O8zQTHh1ypuOzwe25+Nzed8:tMblouyArZDYqXb7s7ETH7cxwV5+8d8

Resources

Icon

Visualization

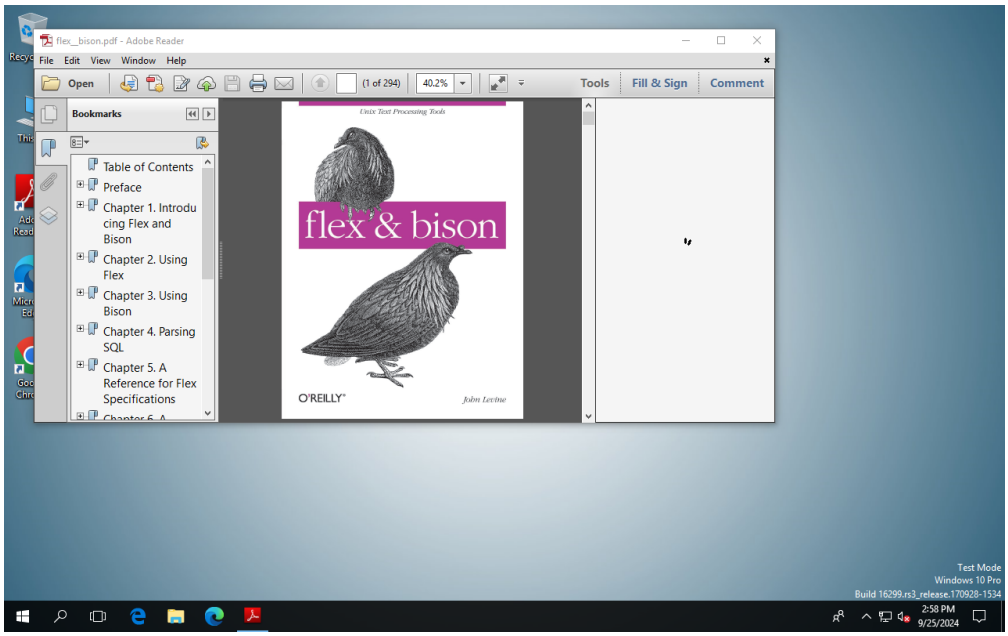
Input File (PortEx)



Classification (TrID)

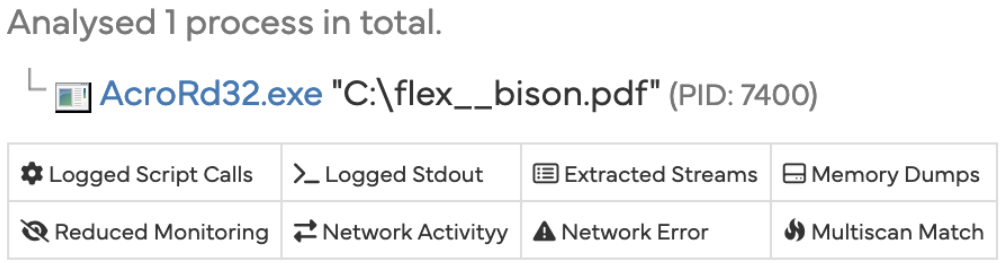
- 100.0% (.PDF) Adobe Portable Document Format

In questo caso, notiamo l'assenza di alcune informazioni che AnyRun ha invece rilevato, come l'anno di creazione del file. Tuttavia, Hybrid Analysis fornisce una **visualizzazione grafica** del file (`visualization`), un aspetto non offerto dagli altri strumenti. Questo è particolarmente interessante, poiché alcune tecniche di rilevamento di malware basate sull'intelligenza artificiale utilizzano proprio la rappresentazione visiva del file per identificare programmi malevoli

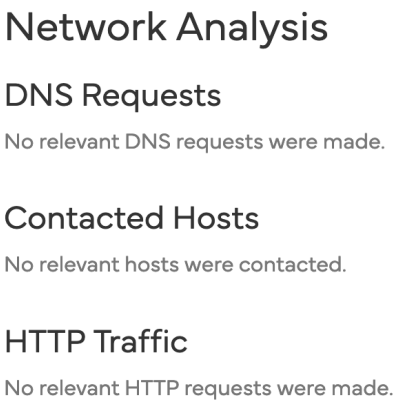


A differenza di AnyRun, il test di Hybrid Analysis è completamente automatizzato e non consente un'interazione diretta con il file. Tuttavia, come possiamo osservare dall'immagine generata nel report, i test eseguiti sono simili a quelli di AnyRun: il sistema operativo

utilizzato è sempre Windows 10 (visibile nella parte inferiore), e il visualizzatore è nuovamente Adobe Reader



In questo caso, è stato analizzato unicamente il processo generato dall'eseguibile *AcroRd32.exe* (presumibilmente una versione di Adobe Reader diversa da quella osservata su AnyRun)



Il report generato da Hybrid Analysis risulta purtroppo più limitato rispetto a quello di AnyRun. Si limita infatti a segnalare che nessun processo e nessuna connessione sono stati ritenuti sospetti, ma non fornisce ulteriori dettagli, come gli indirizzi IP contattati o i sottoprocessi avviati