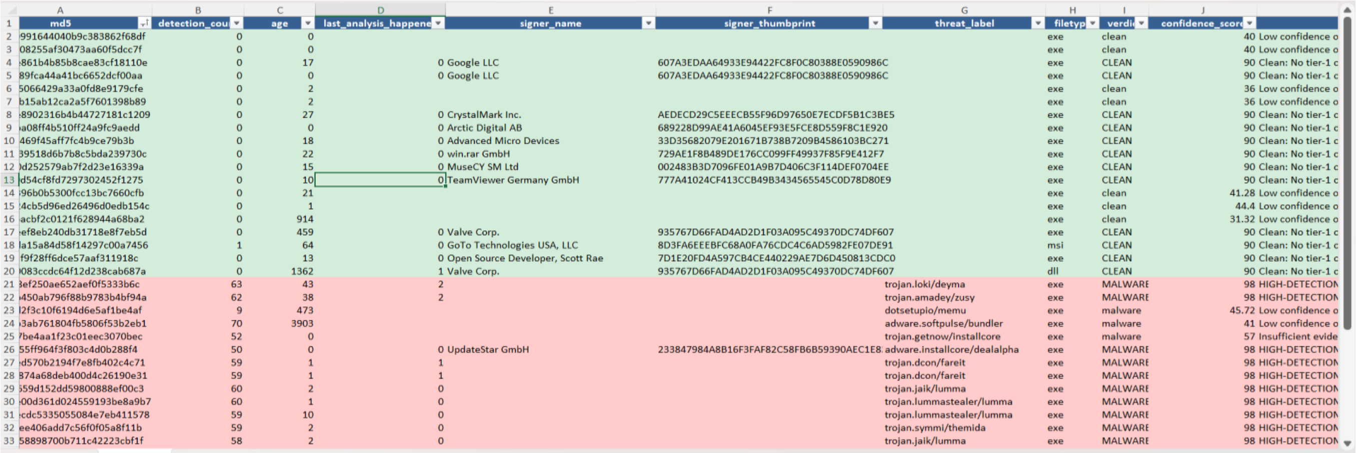
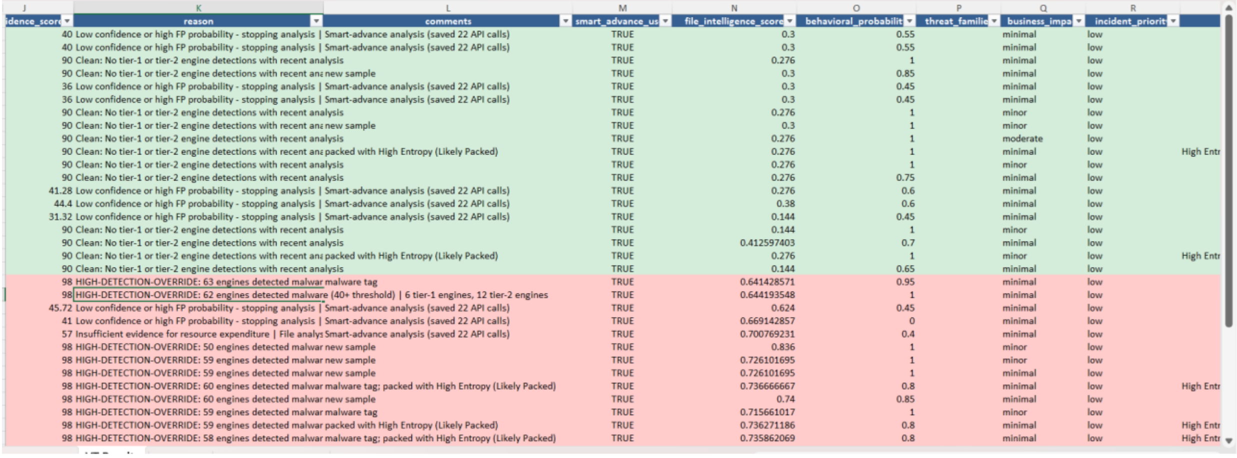
If you use below **cmd** line ,you will get below output and it had columns for analysis and had the color coding ,age of sample ,last analysis in days ,signer info ,verdict and reason etc and many more .

```
python friday_v3_6_13.py download --api-key YOUR_KEY --input md5.txt --smart-advance
```

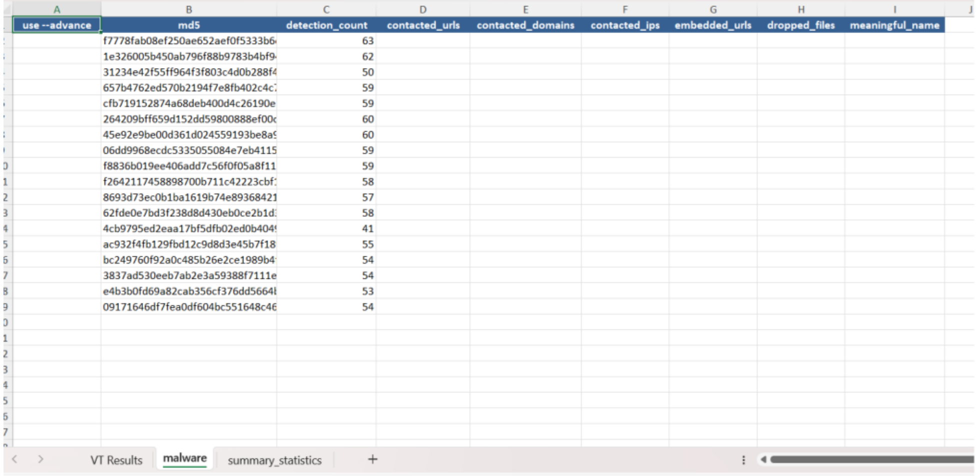


	A	B	C	D	E	F	G	H	I	J	
1	md5	detection_cou	age	last_analysis_happene	signer_name	signer_thumbprint	threat_label	filetyp	verdi	confidence_scor	
2	991644040b9c383862f68df	0	0					exe	clean	40	Low confidence o
3	08255af30473aa60f5dcc7f	0	0					exe	clean	40	Low confidence o
4	861b4b85b8cae83cf18110e	0	17	0	Google LLC	607A3EDAA64933E94422FC8F0C80388E0590986C		exe	CLEAN	90	Clean: No tier-1 c
5	89fca44a41bc6652dcf00aa	0	0	0	Google LLC	607A3EDAA64933E94422FC8F0C80388E0590986C		exe	CLEAN	90	Clean: No tier-1 c
6	5066429a33a0fd8e9179cfe	0	2					exe	clean	36	Low confidence o
7	b15ab12ca2a5f7601398b89	0	2					exe	clean	36	Low confidence o
8	8902316b4b44727181c1209	0	27	0	CrystalMark Inc.	AEDECD29C5EEECB55F96D97650E7ECDF5B1C3BE5		exe	CLEAN	90	Clean: No tier-1 c
9	a08ff4b510ff24a9fc9aedd	0	0	0	Arctic Digital AB	689228D99AE41A6045EF93E5FCE8D559F8C1E920		exe	CLEAN	90	Clean: No tier-1 c
10	469f45aff7fc4b9ce79b3b	0	18	0	Advanced Micro Devices	33D35682079E201671B738B7209B4586103BC271		exe	CLEAN	90	Clean: No tier-1 c
11	39518d6b7b8c5bda239730c	0	22	0	win.rar GmbH	729AE1F8B489DE176CC099FF49937F85F9E412F7		exe	CLEAN	90	Clean: No tier-1 c
12	d252579ab7f2d23e16339a	0	15	0	MuseCY SM Ltd	002483B3D7096FE01A9B7D406C3F114DEF0704EE		exe	CLEAN	90	Clean: No tier-1 c
13	d54cf8fd7297302452f1275	0	10	0	TeamViewer Germany GmbH	777A41024CF413CCB49B3434565545C0D78D80E9		exe	CLEAN	90	Clean: No tier-1 c
14	96b0b5300fcc13bc7660cfb	0	21					exe	clean	41.28	Low confidence o
15	4cb5d96ed26496d0edb154c	0	1					exe	clean	44.4	Low confidence o
16	acbf2c0121f628944a68ba2	0	914					exe	clean	31.32	Low confidence o
17	ef8eb240db31718e8f7eb5d	0	459	0	Valve Corp.	935767D66FAD4AD2D1F03A095C49370DC74DF607		exe	CLEAN	90	Clean: No tier-1 c
18	a15a84d58f14297c00a7456	1	64	0	GoTo Technologies USA, LLC	8D3FA6EEEBFC68A0FA76CDC4C6AD5982FE07DE91		msi	CLEAN	90	Clean: No tier-1 c
19	f9f28ff6dce57aaf311918c	0	13	0	Open Source Developer, Scott Rae	7D1E20FD4A597CB4CE440229AE7D6D450813CDC0		exe	CLEAN	90	Clean: No tier-1 c
20	083ccdc64f12d238cab687a	0	1362	1	Valve Corp.	935767D66FAD4AD2D1F03A095C49370DC74DF607		dll	CLEAN	90	Clean: No tier-1 c
21	ef250ae652aef0f5333b6c	63	43	2			trojan.loki/deyma	exe	MALWARE	98	HIGH-DETECTION
22	450ab796f88b9783b4bf94a	62	38	2			trojan.amadey/zusy	exe	MALWARE	98	HIGH-DETECTION
23	2f3c10f6194d6e5af1be4af	9	473				dotsetupio/memu	exe	malware	45.72	Low confidence o
24	3ab761804fb5806f53b2eb1	70	3903				adware.softpulse/bundler	exe	malware	41	Low confidence o
25	7be4aa1f23c01eec3070bec	52	0				trojan.getnow/installcore	exe	malware	57	Insufficient evide
26	55ff964f3f803c4d0b288f4	50	0	0	UpdateStar GmbH	233847984A8B16F3FAF82C58FB6B59390AEC1E8	adware.installcore/dealalpha	exe	MALWARE	98	HIGH-DETECTION
27	d570b2194f7e8fb402c4c71	59	1	1			trojan.dcon/fareit	exe	MALWARE	98	HIGH-DETECTION
28	874a68deb400d4c26190e31	59	1	1			trojan.dcon/fareit	exe	MALWARE	98	HIGH-DETECTION
29	59d152dd59800888ef00c3	60	2	0			trojan.jaik/lumma	exe	MALWARE	98	HIGH-DETECTION
30	00d361d024559193be8a9b7	60	1	0			trojan.lummastealer/lumma	exe	MALWARE	98	HIGH-DETECTION
31	cdc5335055084e7eb411578	59	10	0			trojan.lummastealer/lumma	exe	MALWARE	98	HIGH-DETECTION
32	ee406add7c56f0f05a8f11b	59	2	0			trojan.symmi/themida	exe	MALWARE	98	HIGH-DETECTION
33	58898700b711c42223cbf1f	58	2	0			trojan.jaik/lumma	exe	MALWARE	98	HIGH-DETECTION



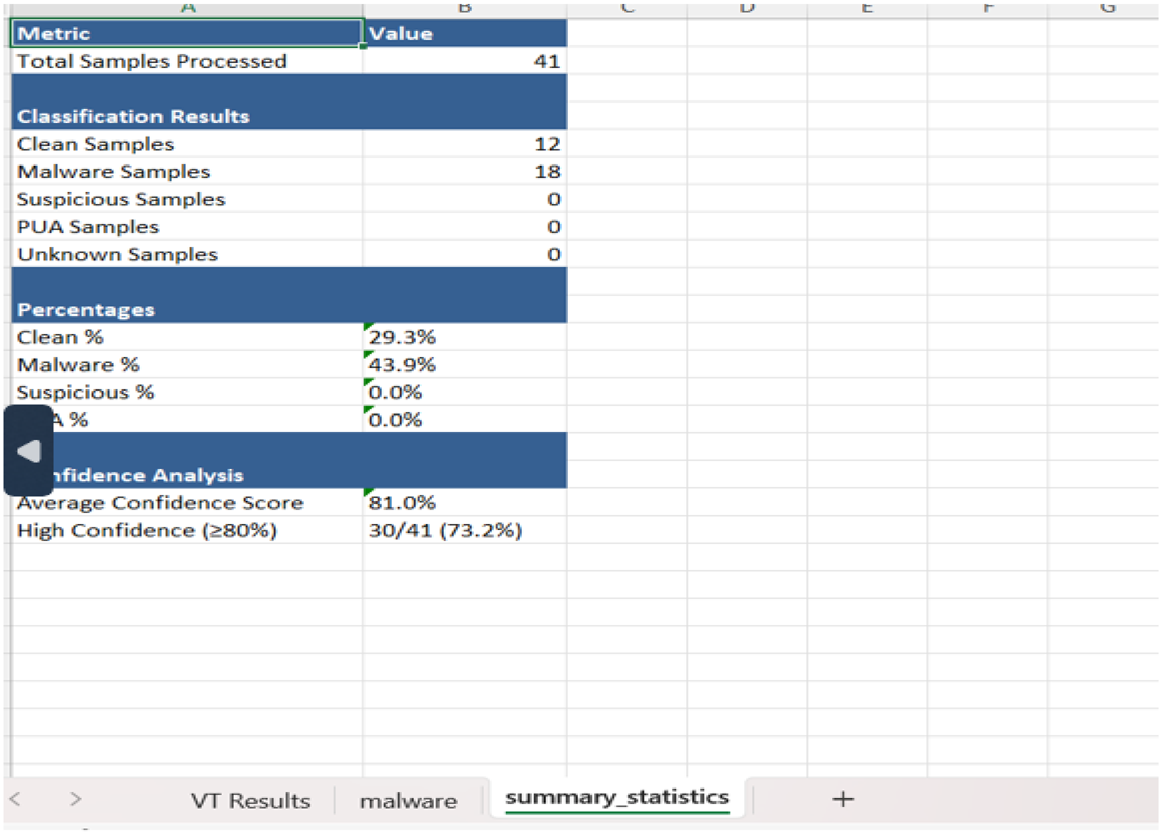
J	K	L	M	N	O	P	Q	R	
idence_score	reason	comments	smart_advance_us	file_intelligence_score	behavioral_probabilit	threat_familie	business_impa	incident_priorit	
40	Low confidence or high FP probability - stopping analysis |	Smart-advance analysis (saved 22 API calls)	TRUE	0.3	0.55		minimal	low	
40	Low confidence or high FP probability - stopping analysis |	Smart-advance analysis (saved 22 API calls)	TRUE	0.3	0.55		minimal	low	
90	Clean: No tier-1 or tier-2 engine detections with recent analysis		TRUE	0.276	1		minimal	low	
90	Clean: No tier-1 or tier-2 engine detections with recent ana	new sample	TRUE	0.3	0.85		minimal	low	
36	Low confidence or high FP probability - stopping analysis |	Smart-advance analysis (saved 22 API calls)	TRUE	0.3	0.45		minimal	low	
36	Low confidence or high FP probability - stopping analysis |	Smart-advance analysis (saved 22 API calls)	TRUE	0.3	0.45		minimal	low	
90	Clean: No tier-1 or tier-2 engine detections with recent analysis		TRUE	0.276	1		minor	low	
90	Clean: No tier-1 or tier-2 engine detections with recent ana	new sample	TRUE	0.3	1		minor	low	
90	Clean: No tier-1 or tier-2 engine detections with recent analysis		TRUE	0.276	1		moderate	low	
90	Clean: No tier-1 or tier-2 engine detections with recent ana	packed with High Entropy (Likely Packed)	TRUE	0.276	1		minimal	low	High Entr
90	Clean: No tier-1 or tier-2 engine detections with recent analysis		TRUE	0.276	1		minor	low	
90	Clean: No tier-1 or tier-2 engine detections with recent analysis		TRUE	0.276	0.75		minimal	low	
41.28	Low confidence or high FP probability - stopping analysis |	Smart-advance analysis (saved 22 API calls)	TRUE	0.276	0.6		minimal	low	
44.4	Low confidence or high FP probability - stopping analysis |	Smart-advance analysis (saved 22 API calls)	TRUE	0.38	0.6		minimal	low	
31.32	Low confidence or high FP probability - stopping analysis |	Smart-advance analysis (saved 22 API calls)	TRUE	0.144	0.45		minimal	low	
90	Clean: No tier-1 or tier-2 engine detections with recent analysis		TRUE	0.144	1		minor	low	
90	Clean: No tier-1 or tier-2 engine detections with recent analysis		TRUE	0.412597403	0.7		minimal	low	
90	Clean: No tier-1 or tier-2 engine detections with recent ana	packed with High Entropy (Likely Packed)	TRUE	0.276	1		minor	low	High Entr
90	Clean: No tier-1 or tier-2 engine detections with recent analysis		TRUE	0.144	0.65		minimal	low	
98	HIGH-DETECTION-OVERRIDE: 63 engines detected malwar	malware tag	TRUE	0.641428571	0.95		minimal	low	
98	HIGH-DETECTION-OVERRIDE: 62 engines detected malware (40+ threshold) | 6 tier-1 engines, 12 tier-2 engines		TRUE	0.644193548	1		minimal	low	
45.72	Low confidence or high FP probability - stopping analysis |	Smart-advance analysis (saved 22 API calls)	TRUE	0.624	0.45		minimal	low	
41	Low confidence or high FP probability - stopping analysis |	Smart-advance analysis (saved 22 API calls)	TRUE	0.669142857	0		minimal	low	
57	Insufficient evidence for resource expenditure | File analys	Smart-advance analysis (saved 22 API calls)	TRUE	0.700769231	0.4		minimal	low	
98	HIGH-DETECTION-OVERRIDE: 50 engines detected malwar	new sample	TRUE	0.836	1		minor	low	
98	HIGH-DETECTION-OVERRIDE: 59 engines detected malwar	new sample	TRUE	0.726101695	1		minor	low	
98	HIGH-DETECTION-OVERRIDE: 59 engines detected malwar	new sample	TRUE	0.726101695	1		minimal	low	
98	HIGH-DETECTION-OVERRIDE: 60 engines detected malwar	malware tag; packed with High Entropy (Likely Packed)	TRUE	0.736666667	0.8		minimal	low	High Entr
98	HIGH-DETECTION-OVERRIDE: 60 engines detected malwar	new sample	TRUE	0.74	0.85		minimal	low	
98	HIGH-DETECTION-OVERRIDE: 59 engines detected malwar	malware tag	TRUE	0.715661017	1		minor	low	
98	HIGH-DETECTION-OVERRIDE: 59 engines detected malwar	packed with High Entropy (Likely Packed)	TRUE	0.736271186	0.8		minimal	low	High Entr
98	HIGH-DETECTION-OVERRIDE: 58 engines detected malwar	malware tag; packed with High Entropy (Likely Packed)	TRUE	0.735862069	0.8		minimal	low	High Entr

It give 3 sheets below it separates for malware



use --advance	md5	detection_count	contacted_urls	contacted_domains	contacted_ips	embedded_urls	dropped_files	meaningful_name
	f7778fab08ef250ae652aef0f5333b6	63						
	1e326005b450ab796f88b9783b4bf9	62						
	31234e42f55ff964f3f803c4d0b288f4	50						
	657b4762ed570b2194f7e8fb402c4c	59						
	cfb719152874a68deb400d4c26190e	59						
	264209bff659d152dd59800888ef00	60						
	45e92e9be00d361d024559193be8a	60						
	06dd9968ecdc5335055084e7eb4115	59						
	f8836b019ee406add7c56f0f05a8f11	59						
	f2642117458898700b711c42223cbf	58						
	8693d73ec0b1ba1619b74e89368421	57						
	62fde0e7bd3f238d8d430eb0ce2b1d	58						
	4cb9795ed2eaa17bf5dfb02ed0b404	41						
	ac932f4fb129fbd12c9d8d3e45b7f18	55						
	bc249760f92a0c485b26e2ce1989b4	54						
	3837ad530eeb7ab2e3a59388f7111e	54						
	e4b3b0fd69a82cab356cf376dd5664	53						
	09171646df7fea0df604bc551648c46	54						

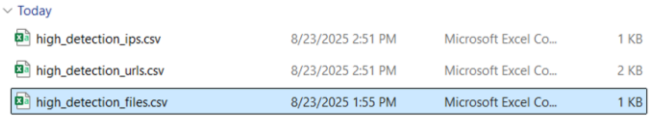
Have executive summary of all samples



Metric	Value
Total Samples Processed	41
Classification Results	
Clean Samples	12
Malware Samples	18
Suspicious Samples	0
PUA Samples	0
Unknown Samples	0
Percentages	
Clean %	29.3%
Malware %	43.9%
Suspicious %	0.0%
A %	0.0%
nfidence Analysis	
Average Confidence Score	81.0%
High Confidence (≥80%)	30/41 (73.2%)

If you use below cmd and it extracts ioc ,it works for when more than 100+ samples

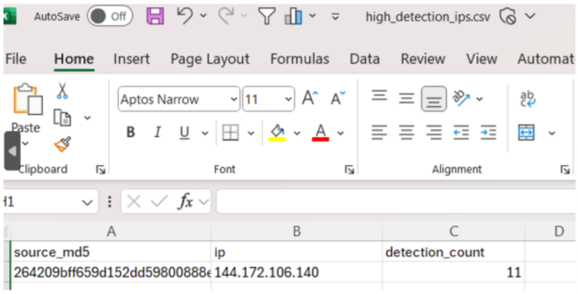
python friday_v3_6_13.py extract --json-dir ./json_files --min-detections 10



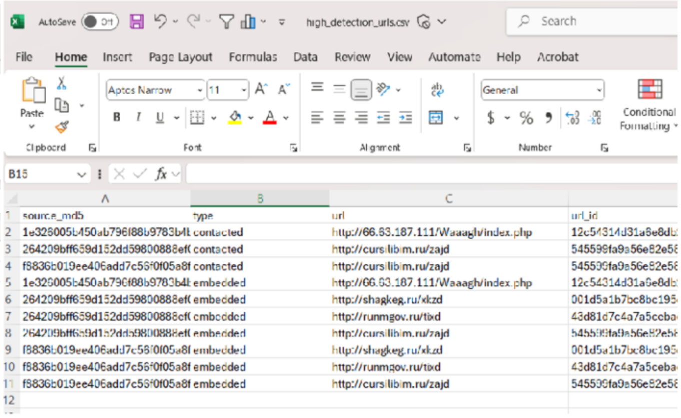
Today

high_detection_ips.csv	8/23/2025 2:51 PM	Microsoft Excel Co...	1 KB
high_detection_urls.csv	8/23/2025 2:51 PM	Microsoft Excel Co...	2 KB
high_detection_files.csv	8/23/2025 1:55 PM	Microsoft Excel Co...	1 KB

we got three files



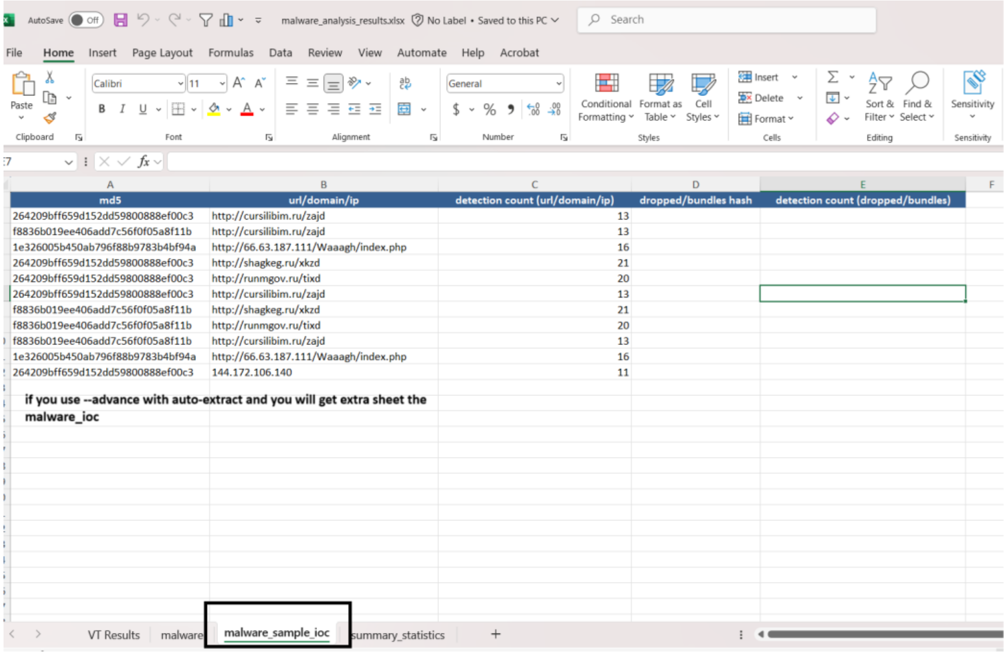
A	B	C
source_md5	ip	detection_count
264209bff659d152dd59800888e	144.172.106.140	11



	A	B	C	
1	source_md5	type	url	url_id
2	1e326005b450ab796f88b9783b4b	contacted	http://66.63.187.111/Waaagh/index.php	12c54314d31a6e8db
3	264209bff659d152dd59800888ef(	contacted	http://cursilibim.ru/zajd	545599fa9a56e82e58
4	f8836b019ee406add7c56f0f05a8f	contacted	http://cursilibim.ru/zajd	545599fa9a56e82e58
5	1e326005b450ab796f88b9783b4b	embedded	http://66.63.187.111/Waaagh/index.php	12c54314d31a6e8db
6	264209bff659d152dd59800888ef(	embedded	http://shagkeg.ru/xkzd	001d5a1b7bc8bc195
7	264209bff659d152dd59800888ef(	embedded	http://runmgov.ru/tixd	43d81d7c4a7a5ceba
8	264209bff659d152dd59800888ef(	embedded	http://cursilibim.ru/zajd	545599fa9a56e82e58
9	f8836b019ee406add7c56f0f05a8f	embedded	http://shagkeg.ru/xkzd	001d5a1b7bc8bc195
10	f8836b019ee406add7c56f0f05a8f	embedded	http://runmgov.ru/tixd	43d81d7c4a7a5ceba
11	f8836b019ee406add7c56f0f05a8f	embedded	http://cursilibim.ru/zajd	545599fa9a56e82e58
12				

The --advance aurgement uses 24 api for each beaware and it will give rich info sample and help full writing signature it detected url ,domain and bundle files and there detections

python friday_v3_6_13.py download --api-key YOUR_KEY --input malware.txt --advance --auto-extract



md5	url/domain/ip	detection count (url/domain/ip)	dropped/bundles hash	detection count (dropped/bundles)
264209bff659d152dd59800888ef00c3	http://cursilibim.ru/zajd	13		
f8836b019ee406add7c56f0f05a8f11b	http://cursilibim.ru/zajd	13		
1e326005b450ab796f88b9783b4bf94a	http://66.63.187.111/Waaagh/index.php	16		
264209bff659d152dd59800888ef00c3	http://shagkeg.ru/xkzd	21		
264209bff659d152dd59800888ef00c3	http://runmgov.ru/tixd	20		
264209bff659d152dd59800888ef00c3	http://cursilibim.ru/zajd	13		
f8836b019ee406add7c56f0f05a8f11b	http://shagkeg.ru/xkzd	21		
f8836b019ee406add7c56f0f05a8f11b	http://runmgov.ru/tixd	20		
f8836b019ee406add7c56f0f05a8f11b	http://cursilibim.ru/zajd	13		
1e326005b450ab796f88b9783b4bf94a	http://66.63.187.111/Waaagh/index.php	16		
264209bff659d152dd59800888ef00c3	144.172.106.140	11		

if you use --advance with auto-extract and you will get extra sheet the malware_ioc

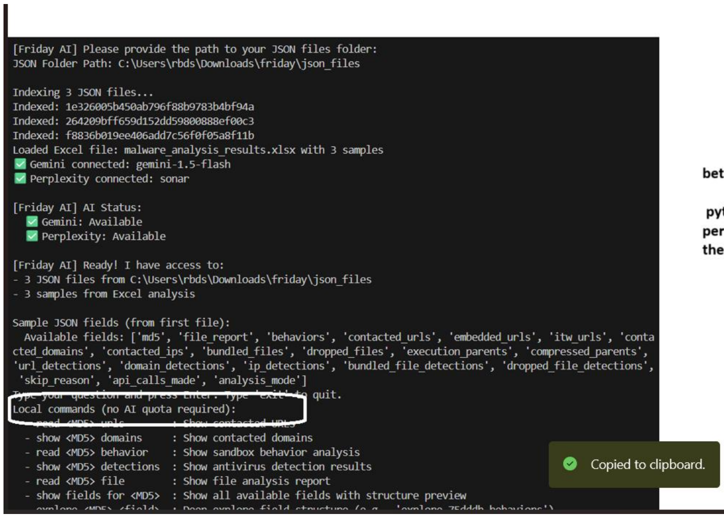
Beta ai features :

# Interactive AI Q&A with Gemini (voice enabled)

python friday_v3_6_13.py speak --speak --gemini-api-key YOUR_GEMINI_KEY

# Interactive AI Q&A with both Gemini and Perplexity (smart routing)

python friday_v3_6_13.py speak --gemini-api-key YOUR_GEMINI_KEY --perplexity-api-key YOUR_PERPLEXITY_KEY

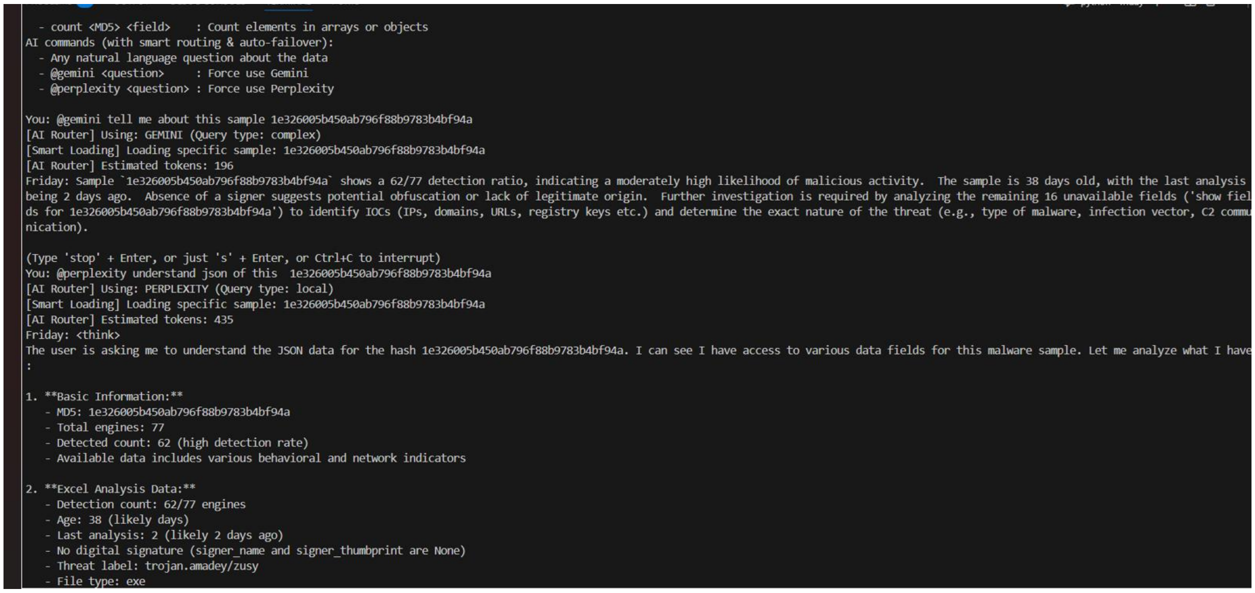


```
[Friday AI] Please provide the path to your JSON files folder:
JSON Folder Path: C:\Users\rbds\Downloads\friday\json_files

Indexing 3 JSON files...
Indexed: 1e326005b450ab796f88b9783b4bf94a
Indexed: 264209bff659d152dd59800888ef00c3
Indexed: f8836b019ee406add7c56f0f05a8f11b
Loaded Excel file: malware_analysis_results.xlsx with 3 samples
✅ Gemini connected: gemini-1.5-flash
✅ Perplexity connected: sonar

[Friday AI] AI Status:
  ✅ Gemini: Available
  ✅ Perplexity: Available

[Friday AI] Ready! I have access to:
- 3 JSON files from C:\Users\rbds\Downloads\friday\json_files
- 3 samples from Excel analysis

Sample JSON fields (from first file):
  Available fields: ['md5', 'file_report', 'behaviors', 'contacted_urls', 'embedded_urls', 'itw_urls', 'conta
cted_domains', 'contacted_ips', 'bundled_files', 'dropped_files', 'execution_parents', 'compressed_parents',
'url_detections', 'domain_detections', 'ip_detections', 'bundled_file_detections', 'dropped_file_detections',
 'skip_reason', 'api_calls_made', 'analysis_mode']
Type your question and press Enter. Type 'exit' to quit.
Local commands (no AI quota required):
  - read <MD5> urls         : Show contacted URLs
  - show <MD5> domains      : Show contacted domains
  - read <MD5> behavior     : Show sandbox behavior analysis
  - show <MD5> detections   : Show antivirus detection results
  - read <MD5> file         : Show file analysis report
  - show fields for <MD5>   : Show all available fields with structure preview
  - explore <MD5> <field>   : Deep explore field structure (e.g., 'explore 75dddb behaviors')
```

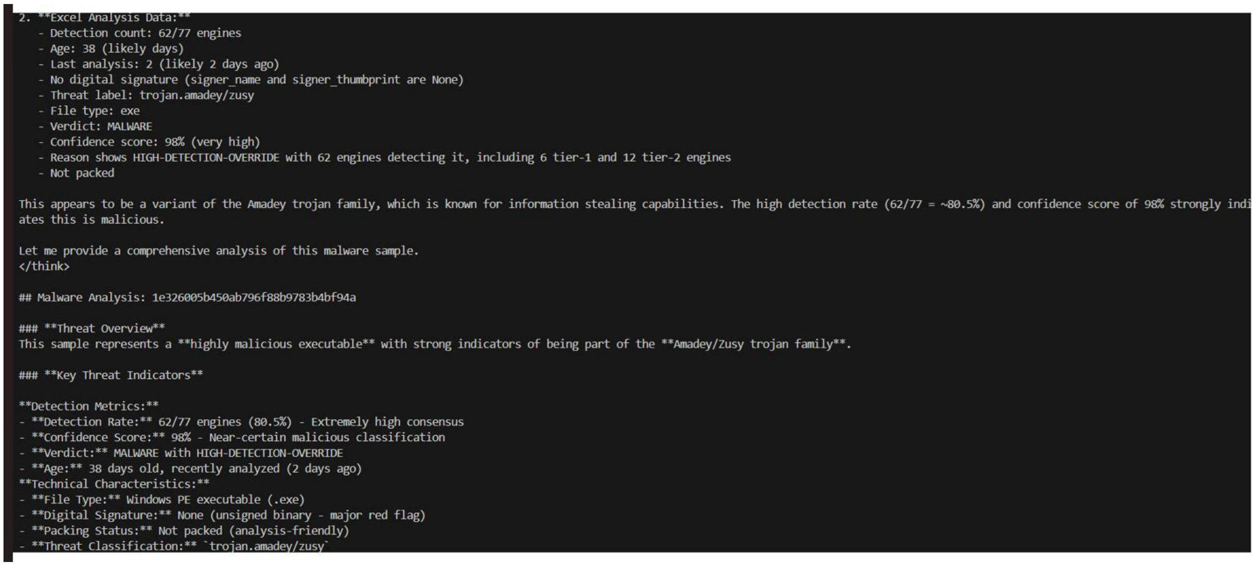
beta feature

python friday_v3_6_13.py speak --speak --gemini-api-key YOUR_GEMINI_KEY --perplexity-api-key YOUR_PERPLEXITY_KEY ----- it can speak out the result and it have local command if you run out ai quota

It can speak and explain about the samples



```
  - count <MD5> <field>    : Count elements in arrays or objects
AI commands (with smart routing & auto-failover):
  - Any natural language question about the data
  - @gemini <question>     : Force use Gemini
  - @perplexity <question> : Force use Perplexity

You: @gemini tell me about this sample 1e326005b450ab796f88b9783b4bf94a
[AI Router] Using: GEMINI (Query type: complex)
[Smart Loading] Loading specific sample: 1e326005b450ab796f88b9783b4bf94a
[AI Router] Estimated tokens: 196
Friday: Sample `1e326005b450ab796f88b9783b4bf94a` shows a 62/77 detection ratio, indicating a moderately high likelihood of malicious activity.  The sample is 38 days old, with the last analysis
being 2 days ago.  Absence of a signer suggests potential obfuscation or lack of legitimate origin.  Further investigation is required by analyzing the remaining 16 unavailable fields ('show fiel
ds for 1e326005b450ab796f88b9783b4bf94a') to identify IOCs (IPs, domains, URLs, registry keys etc.) and determine the exact nature of the threat (e.g., type of malware, infection vector, C2 commu
nication).

(Type 'stop' + Enter, or just 's' + Enter, or Ctrl+C to interrupt)
You: @perplexity understand json of this  1e326005b450ab796f88b9783b4bf94a
[AI Router] Using: PERPLEXITY (Query type: local)
[Smart Loading] Loading specific sample: 1e326005b450ab796f88b9783b4bf94a
[AI Router] Estimated tokens: 435
Friday: <think>
The user is asking me to understand the JSON data for the hash 1e326005b450ab796f88b9783b4bf94a. I can see I have access to various data fields for this malware sample. Let me analyze what I have
:

1. **Basic Information:**
   - MD5: 1e326005b450ab796f88b9783b4bf94a
   - Total engines: 77
   - Detected count: 62 (high detection rate)
   - Available data includes various behavioral and network indicators

2. **Excel Analysis Data:**
   - Detection count: 62/77 engines
   - Age: 38 (likely days)
   - Last analysis: 2 (likely 2 days ago)
   - No digital signature (signer_name and signer_thumbprint are None)
   - Threat label: trojan.amadey/zusy
   - File type: exe
```



```
2. **Excel Analysis Data:**
   - Detection count: 62/77 engines
   - Age: 38 (likely days)
   - Last analysis: 2 (likely 2 days ago)
   - No digital signature (signer_name and signer_thumbprint are None)
   - Threat label: trojan.amadey/zusy
   - File type: exe
   - Verdict: MALWARE
   - Confidence score: 98% (very high)
   - Reason shows HIGH-DETECTION-OVERRIDE with 62 engines detecting it, including 6 tier-1 and 12 tier-2 engines
   - Not packed

This appears to be a variant of the Amadey trojan family, which is known for information stealing capabilities. The high detection rate (62/77 = ~80.5%) and confidence score of 98% strongly indi
ates this is malicious.

Let me provide a comprehensive analysis of this malware sample.
</think>

## Malware Analysis: 1e326005b450ab796f88b9783b4bf94a

### **Threat Overview**
This sample represents a **highly malicious executable** with strong indicators of being part of the **Amadey/Zusy trojan family**.

### **Key Threat Indicators**

**Detection Metrics:**
- **Detection Rate:** 62/77 engines (80.5%) - Extremely high consensus
- **Confidence Score:** 98% - Near-certain malicious classification
- **Verdict:** MALWARE with HIGH-DETECTION-OVERRIDE
- **Age:** 38 days old, recently analyzed (2 days ago)
**Technical Characteristics:**
- **File Type:** Windows PE executable (.exe)
- **Digital Signature:** None (unsigned binary - major red flag)
- **Packing Status:** Not packed (analysis-friendly)
- **Threat Classification:** `trojan.amadey/zusy`
```

It had local also command once you ai quota done

Note :

It has more capabilities than which I mentioned earlier , try the tool and it had multiple arguments to explore ,goal is to help and speed the bulk analysis of samples which available in VT