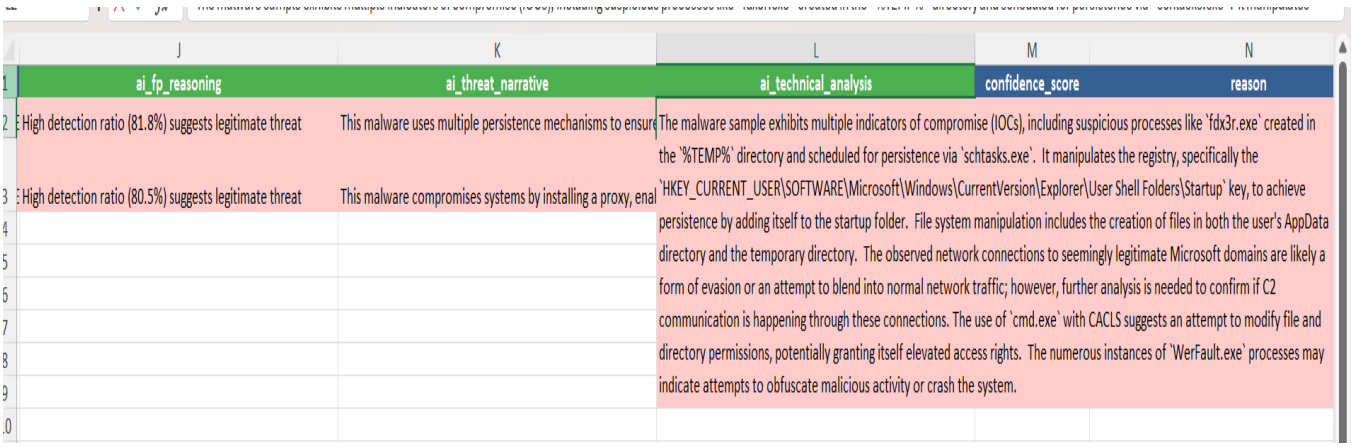
```
usage: friday_with_icon.exe [-h] [--speak] {download,extract,speak} ...

Complete Enhanced VirusTotal Enterprise API Tool with Advanced Classification

positional arguments:
  {download,extract,speak}
                        Operation mode
    download            Download data from VirusTotal API and classify
    extract             Extract indicators from existing JSON files
    speak               Interactive AI Q&A with TTS (supports Gemini + Perplexity)

options:
  -h, --help            show this help message and exit
  --speak               Enable interactive natural language Q&A with spoken answers (requires pyttsx3).

Available Arguments:

DOWNLOAD MODE:
  --api-key KEY           VirusTotal API key (required)
  --input FILE            Input file with MD5 hashes (default: md5.txt)
  --json-dir DIR          Directory to save JSON files (default: json_files)
  --auto-extract          Auto-extract IOCs for malware samples
  --min-detections N      Min detection count for IOC extraction (default: 5)
  --output-dir DIR        Output directory for CSV files (default: extracted_data)
  --output-json FILE      Output JSON file (default: extracted_summary.json)
  --excel-output FILE     Excel output filename (default: virustotal_enhanced_analysis_results.xlsx)
  --rate-limit SECONDS    Rate limit between requests (default: 15.0)
  --advance               Enable advanced analysis (behavioral data, relationships)
  --skip-extended         Skip extended analysis for clean/old/PUA samples (optimization)
  --api-count             Include API call count in Excel output
  --ai                    Enable AI-powered analysis (requires --gemini-api-key or --perplexity-api-key)
  --gemini-api-key KEY    Google Gemini API key for AI features
  --smart-advance         Enable smart-advance mode (5-layer intelligence, 2 API calls per sample)

EXTRACT MODE:
  --json-dir DIR          Directory with JSON files (default: json_files)
  --output-dir DIR        Output directory for CSV files (default: extracted_data)
  --output-json FILE      Output JSON file (default: extracted_summary.json)
  --min-detections N      Minimum detection count (default: 5)

SPEAK MODE (Interactive AI Q&A):
  --json-folder DIR       Directory with JSON files for analysis (default: json_files)
  --gemini-api-key KEY    Google Gemini API key for AI responses
  --perplexity-api-key KEY Perplexity Pro API key for advanced threat intelligence

Analysis Modes:
1. Basic Mode (default): Only file report analysis (1 API call per sample)
2. Advanced Mode (--advance): Full relationship analysis + behavioral data
3. Auto-extract: Works with file report only (use with --advance for full IOC extraction)
```

	md5	detection_count	age	last_analysis_happened	signer_name	signer_thumbprint	threat_label	filetype	verdict	confidence_score	
2	ca5407720991644040b9c383862f68df	0	0					exe	clean	40	Low confidenc
3	41c6c6d5b08255af30473aa60f5dcc7f	0	0					exe	clean	40	Low confidenc
4	de651827e861b4b85b8cae83cf18110e	0	17	0	Google LLC	607A3EDAA64933E94422FC8F0C80388E0590986C		exe	CLEAN	90	Clean: No tier-
5	b6b0dfe2989fca44a41bc6652dcf00aa	0	0	0	Google LLC	607A3EDAA64933E94422FC8F0C80388E0590986C		exe	CLEAN	90	Clean: No tier-
6	f7778fab08ef250ae652aef0f5333b6c	63	43	2			trojan.loki/deyma	exe	MALWARE	98	HIGH-DETECTI
7	1e326005b450ab796f88b9783b4bf94a	62	38	2			trojan.amadey/zusy	exe	MALWARE	98	HIGH-DETECTI
8	bfdc531905066429a33a0fd8e9179cfe	0	2					exe	clean	36	Low confidenc
9	34a6edb2d2f3c10f6194d6e5af1be4af	9	473				dotsetupio/memu	exe	malware	45.72	Low confidenc
10	56fe91833b15ab12ca2a5f7601398b89	0	2					exe	clean	36	Low confidenc
11	0226a27bb3ab761804fb5806f53b2eb1	70	3903				adware.softpulse/bundler	exe	malware	41	Low confidenc
12	eff061a577be4aa1f23c01eec3070bec	52	0				trojan.getnow/installcore	exe	malware	57	Insufficient evi
13	31234e42f55ff964f3f803c4d0b288f4	50	0	0	UpdateStar GmbH	233847984A8B16F3FAF82C58FB6B59390AEC1E8	adware.installcore/dealalpha	exe	MALWARE	98	HIGH-DETECTI
14	657b4762ed570b2194f7e8fb402c4c71	59	1	1			trojan.dcon/fareit	exe	MALWARE	98	HIGH-DETECTI
15	cfb719152874a68deb400d4c26190e31	59	1	1			trojan.dcon/fareit	exe	MALWARE	98	HIGH-DETECTI
16	264209bff659d152dd59800888ef00c3	60	2	0			trojan.jaik/lumma	exe	MALWARE	98	HIGH-DETECTI
17	45e92e9be00d361d024559193be8a9b7	60	1	0			trojan.lummastealer/lumma	exe	MALWARE	98	HIGH-DETECTI
18	06dd9968ecdc5335055084e7eb411578	59	10	0			trojan.lummastealer/lumma	exe	MALWARE	98	HIGH-DETECTI
19	f8836b019ee406add7c56f0f05a8f11b	59	2	0			trojan.symmi/themida	exe	MALWARE	98	HIGH-DETECTI
20	f26421174588987 00b711c42223cbf1f	58	2	0			trojan.jaik/lumma	exe	MALWARE	98	HIGH-DETECTI
21	8693d73ec0b1ba1619b74e8936842123	57	2	0			trojan.injectornett/lazy	exe	MALWARE	98	HIGH-DETECTI
22	62fde0e7bd3f238d8d430eb0ce2b1d3f	58	2	0			trojan.symmi/themida	exe	MALWARE	98	HIGH-DETECTI
23	4cb9795ed2eaa17bf5dfb02ed0b4049b	41	3	0			trojan.runner/autoit	exe	MALWARE	98	HIGH-DETECTI
24	ac932f4fb129fbd12c9d8d3e45b7f189	55	3	0			trojan.runner/nsis	exe	MALWARE	98	HIGH-DETECTI
25	bc249760f92a0c485b26e2ce1989b4fb	54	2	0	NVIDIA Corporation	15F760D82C79D22446CC7D4806540BF632B1E1(	trojan.lazy/krypt	exe	MALWARE	98	HIGH-DETECTI
26	c7f59a0a1482314d12219ee225426585	54	3				trojan.redcap/rhadamanthys	exe	malware	63	Insufficient evi
27	3837ad530eeb7ab2e3a59388f7111ea1	54	3	0	NVIDIA Corporation	15F760D82C79D22446CC7D4806540BF632B1E1(	trojan.krypt/injectornett	exe	MALWARE	98	HIGH-DETECTI
28	e4b3b0fd69a82cab356cf376dd5664bb	53	2	0	Open Source Developer, Dominik Reichl	A7630D3DA78F342F60EA0B0076269B554BEE398	trojan.razy/amadey	exe	MALWARE	98	HIGH-DETECTI
29	09171646df7fea0df604bc551648c461	54	2	0	Open Source Developer, Dominik Reichl	A7630D3DA78F342F60EA0B0076269B554BEE398	trojan.razy/sbescape	exe	MALWARE	98	HIGH-DETECTI
30	16a15552e8902316b4b44727181c1209	0	27	0	CrystalMark Inc.	AEDECD29C5EEECB55F96D97650E7ECDF5B1C3BE5		exe	CLEAN	90	Clean: No tier-
31	edd60331ba08ff4b510ff24a9fc9aedd	0	0	0	Arctic Digital AB	689228D99AE41A6045EF93E5FCE8D559F8C1E920		exe	CLEAN	90	Clean: No tier-
32	9cf9f5df5d469f45aff7fc4b9ce79b3b	0	18	0	Advanced Micro Devices	33D35682079E201671B738B7209B4586103BC271		exe	CLEAN	90	Clean: No tier-
33	4ecf0ad9b39518d6b7b8c5bda239730c	0	22	0	win.rar GmbH	729AE1F8B489DE176CC099FF49937F85F9E412F7		exe	CLEAN	90	Clean: No tier-

VT Results | malware | summary_statistics | +

	reason	comments	smart_advance_used	file_intelligence_score	behavioral_probability	threat_families	business_impact	ir
2	Low confidence or high FP probability - stopping analysis | Be	Smart-advance analysis (saved 22 API calls)	TRUE	0.3	0.55		minimal	low
3	Low confidence or high FP probability - stopping analysis | Be	Smart-advance analysis (saved 22 API calls)	TRUE	0.3	0.55		minimal	low
4	Clean: No tier-1 or tier-2 engine detections with recent analysis		TRUE	0.276	1		minimal	low
5	Clean: No tier-1 or tier-2 engine detections with recent analy	new sample	TRUE	0.3	0.85		minimal	low
6	HIGH-DETECTION-OVERRIDE: 63 engines detected malware (	malware tag	TRUE	0.641428571	0.95		minimal	low
7	HIGH-DETECTION-OVERRIDE: 62 engines detected malware (40+ threshold) | 6 tier-1 engines, 12 tier-2 engines		TRUE	0.644193548	1		minimal	low
8	Low confidence or high FP probability - stopping analysis | Be	Smart-advance analysis (saved 22 API calls)	TRUE	0.3	0.45		minimal	low
9	Low confidence or high FP probability - stopping analysis | Fil	Smart-advance analysis (saved 22 API calls)	TRUE	0.624	0.45		minimal	low
10	Low confidence or high FP probability - stopping analysis | Be	Smart-advance analysis (saved 22 API calls)	TRUE	0.3	0.45		minimal	low
11	Low confidence or high FP probability - stopping analysis | Fil	Smart-advance analysis (saved 22 API calls)	TRUE	0.669142857	0		minimal	low
12	Insufficient evidence for resource expenditure | File analysis:	Smart-advance analysis (saved 22 API calls)	TRUE	0.700769231	0.4		minimal	low
13	HIGH-DETECTION-OVERRIDE: 50 engines detected malware (	new sample	TRUE	0.836	1		minor	low
14	HIGH-DETECTION-OVERRIDE: 59 engines detected malware (	new sample	TRUE	0.726101695	1		minor	low
15	HIGH-DETECTION-OVERRIDE: 59 engines detected malware (	new sample	TRUE	0.726101695	1		minimal	low
16	HIGH-DETECTION-OVERRIDE: 60 engines detected malware (	malware tag; packed with High Entropy (Likely Packed)	TRUE	0.736666667	0.8		minimal	low
17	HIGH-DETECTION-OVERRIDE: 60 engines detected malware (	new sample	TRUE	0.74	0.85		minimal	low
18	HIGH-DETECTION-OVERRIDE: 59 engines detected malware (	malware tag	TRUE	0.715661017	1		minor	low
19	HIGH-DETECTION-OVERRIDE: 59 engines detected malware (	packed with High Entropy (Likely Packed)	TRUE	0.736271186	0.8		minimal	low
20	HIGH-DETECTION-OVERRIDE: 58 engines detected malware (	malware tag; packed with High Entropy (Likely Packed)	TRUE	0.735862069	0.8		minimal	low
21	HIGH-DETECTION-OVERRIDE: 57 engines detected malware (	packed with High Entropy (Likely Packed)	TRUE	0.728421053	1		minor	low
22	HIGH-DETECTION-OVERRIDE: 58 engines detected malware (	malware tag; packed with High Entropy (Likely Packed)	TRUE	0.735862069	0.8		minimal	low
23	HIGH-DETECTION-OVERRIDE: 41 engines detected malware (40+ threshold) | 4 tier-1 engines, 11 tier-2 engines		TRUE	0.740487805	1		minor	low
24	HIGH-DETECTION-OVERRIDE: 55 engines detected malware (	packed with High Entropy (Likely Packed)	TRUE	0.738181818	1		minor	low
25	HIGH-DETECTION-OVERRIDE: 54 engines detected malware (	packed with High Entropy (Likely Packed)	TRUE	0.83037037	1		minor	low
26	Insufficient evidence for resource expenditure | File analysis:	Smart-advance analysis (saved 22 API calls)	TRUE	0.69037037	0.55		minimal	low
27	HIGH-DETECTION-OVERRIDE: 54 engines detected malware (	packed with High Entropy (Likely Packed)	TRUE	0.83037037	1		minor	low

VT Results | malware | summary_statistics | +



	J	K	L	M	N
1	ai_fp_reasoning	ai_threat_narrative	ai_technical_analysis	confidence_score	reason
2	High detection ratio (81.8%) suggests legitimate threat	This malware uses multiple persistence mechanisms to ensure	The malware sample exhibits multiple indicators of compromise (IOCs), including suspicious processes like `fdx3r.exe` created in the `%TEMP%` directory and scheduled for persistence via `schtasks.exe`. It manipulates the registry, specifically the `HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Startup` key, to achieve persistence by adding itself to the startup folder. File system manipulation includes the creation of files in both the user's AppData directory and the temporary directory. The observed network connections to seemingly legitimate Microsoft domains are likely a form of evasion or an attempt to blend into normal network traffic; however, further analysis is needed to confirm if C2 communication is happening through these connections. The use of `cmd.exe` with CACLS suggests an attempt to modify file and directory permissions, potentially granting itself elevated access rights. The numerous instances of `WerFault.exe` processes may indicate attempts to obfuscate malicious activity or crash the system.		
3	High detection ratio (80.5%) suggests legitimate threat	This malware compromises systems by installing a proxy, enal			
4					
5					
6					
7					
8					
9					
10					

1	ai_fp_reasoning	ai_threat_narrative	ai_technical_analysis	confidence_score	reason
2	High detection ratio (81.8%) suggests legitimate threat	This malware uses multiple persistence mechanisms to ensure	The malware sample exhibits multiple indicators of comprom	98	HIGH-DETECTION-OVERRIDE: 63 engines detec
3	High detection ratio (80.5%) suggests legitimate threat	This malware compromises systems by installing a proxy, ena	The malware sample, identified by MD5 hash 1e326005b450ab796f88b9783b4bf94a, exhibits several concerning behaviors. The suspicious process `nudwee.exe`, dropped in the `%TEMP%` directory, suggests a potential information-stealing or remote access trojan. The malware modifies the registry to set a proxy server (`%HTTP_PROXY%:8080`), potentially to hide its communication with the C2 servers at IPs `66.63.187.111` and `77.246.106.30`. Persistence is achieved by creating a scheduled task (`nudwee.job`), ensuring execution even after a system restart. File operations suggest the malware's attempts to write and access files in various locations, indicating data exfiltration or further malicious actions.		
4					
5					
6					
7					
8					
9					