SemanticsAV

An Edge-to-Cloud AI Foundation
for Instantaneous and Explainable Threat Intelligence

https://www.semanticsav.ai/

A Rigged Game

Static Analysis: Syntax Without Semantics

Precision vs Progress

Core Limitation:

Analyzes what code looks like, not what it means

Dynamic Sandbox: The Execution Trap

Observation vs Authenticity

Core Limitation:

Costly execution buys a show the malware directs

Tradition AI/ML: The Black Box

Power vs Trust

Core Limitation:

Delivers verdicts without verifiable evidence or reasoning

A Rigged Game

Static Analysis: Syntax Without Semantics

Precision vs Progress

Core Limitation:

Analyzes what code looks like, not what it means

- ✕ Fear of false positives restricts detection to the already know
- ✕ Reactive by design, a signature is created only after the damage is done
- ✕ It analyzes appearance (syntax), completely blind to intent (semantics)
- ✕ The slightest obfuscation shatters the model, forcing an endless cycle of updates

Tradition AI/ML: The Black Box

Power vs Trust

Core Limitation:

Delivers verdicts without verifiable evidence or reasoning

A Rigged Game

Dynamic Sandbox: The Execution Trap

Observation vs Authenticity

Core Limitation:

Costly execution buys a show the malware directs

- ✕ Organizations accept the cost because execution promises to reveal true behavior
- ✕ Minutes per sample creates bottlenecks incompatible with real-time protection
- ✕ Full file uploads consume vast bandwidth, imposing strict size limits
- ✕ VM detection and time delays trigger benign behavior, bypassing observation completely

A Rigged Game

Static Analysis: Syntax Without Semantics

Precision vs Progress

Core Limitation:

Analyzes what code looks like, not what it means

Traditional AI/ML: The Black Box

Power vs Trust

Core Limitation:

Delivers verdicts without verifiable evidence or reasoning

- ✕ High detection rates seduce organizations into deploying models they cannot understand
- ✕ Opacity forces a binary choice between blind trust and complete rejection
- ✕ No path from verdict to evidence leaves every decision unverifiable
- ✕ Analysts waste time questioning the system rather than hunting threats

So the real question becomes...

Can we escape the trade-offs?

Imagine threat intelligence with:

- No signatures to maintain
- No hand-crafted rules to tune
- No chasing after threat
- No sandbox theater or waiting
- No blind trust in black-boxes

Attackers shift shape

Defense must understand structure

Beyond Trade-Offs

Zero-Day Detection: Architecture Over Signatures

Coverage AND precision

The Foundation:

AI discovers patterns invisible to human experts

Verifiable Intelligence: Evidence Over Verdicts

Power WITH Transparency

The Foundation:

Geometric position explains the 'why' behind every verdict

Threat Attribution: Lineage Over Labels

Identity AND Ecosystem

The Foundation:

Architectural DNA reveals genetic lineage

Beyond Trade-Offs

Zero-Day Detection: Architecture Over Signatures

Coverage AND precision

The Foundation:

AI discovers patterns invisible to human experts

- ✓ End-to-end learning from raw binaries eliminates all human bias
- ✓ Opaque detection model achieves pattern recognition impossible through manual design
- ✓ Heavy obfuscation produces distinctive patterns that strengthen detection accuracy
- ✓ Architectural pattern generalization detects threat variants without signature updates

Threat Attribution: Lineage Over Labels

Identity AND Ecosystem

The Foundation:

Architectural DNA reveals genetic lineage

Beyond Trade-Offs

Verifiable Intelligence: Evidence Over Verdicts

Power WITH Transparency

The Foundation:

Geometric position explains the ‘why’ behind every verdict

- ✓ Every file positioned against complete code universe
- ✓ Verdict-independent positioning provides parallel validation unconstrained by detection results
- ✓ Geometric neighbors reveal architectural similarities the detection model observed
- ✓ Unfiltered positioning regardless of verdict transforms transparency into confidence metrics

Beyond Trade-Offs

Zero-Day Detection: Architecture Over Signatures

Coverage AND precision

The Foundation:

AI discovers patterns invisible to human experts

Threat Attribution: Lineage Over Labels

Identity AND Ecosystem

The Foundation:

Architectural DNA reveals genetic lineage

- ✓ Identical architecture produces identical DNA regardless of obfuscation or rebranding
- ✓ Genetic positioning maps each sample to specific threat families in code universe
- ✓ Evolutionary branching patterns trace how threats mutate and rebrand across campaigns
- ✓ Genetic relationships map isolated threats into interconnected campaign ecosystem

SemanticsAV Overview

Offline SDK

- Zero-Day Protection
- Offline Complete
- Signature-Free

Cloud Intelligence

- Payload-Only Privacy
- Threat DNA Mapping
- Geometric Proof

Transparent CLI

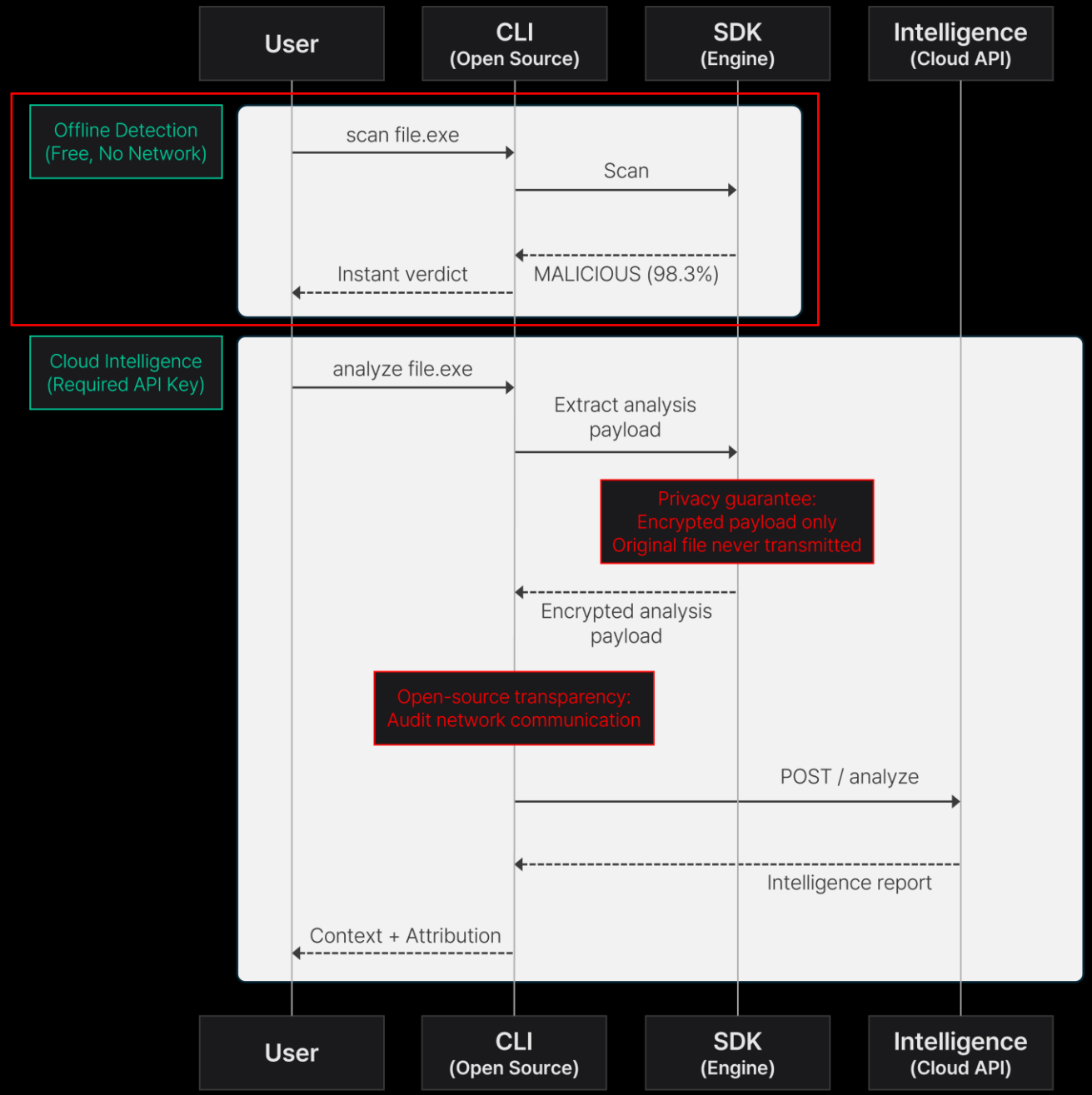
- MIT-licensed
- Auditable open source
- Exclusive network handler

Offline SDK

AI-native detection without signatures or network dependency.

Zero-day protection through architectural pattern recognition; no cloud connection, no compromise.

Complete malware detection in every air-gapped deployment.

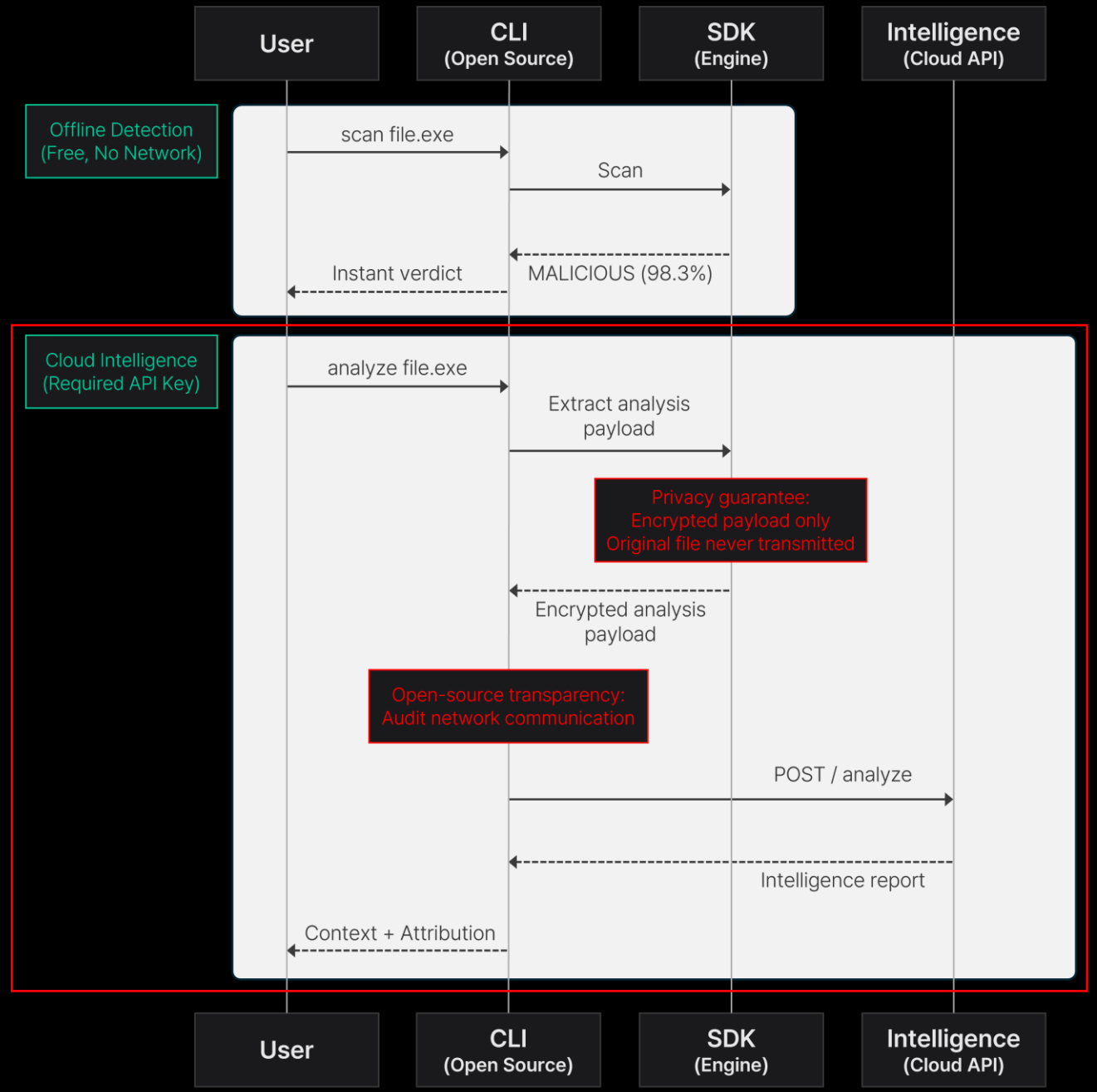


Cloud Intelligence

Threat ecosystem mapping without exposing the file.

Non-reconstructible architectural fingerprinting — positions every sample in the global malware landscape.

Family attribution, campaign correlation, and geometric similarity, instantly.

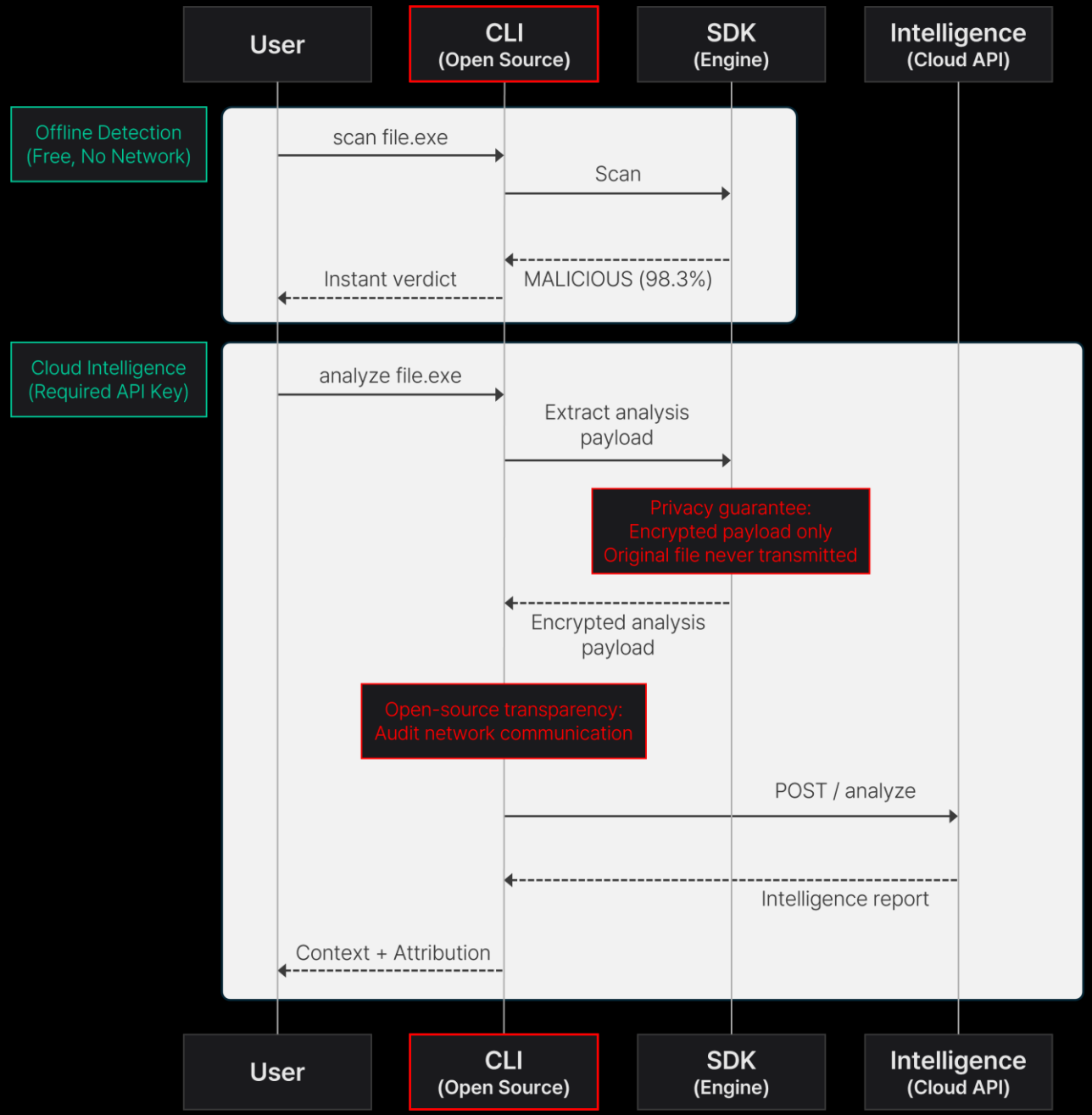


Transparent CLI

Transparency through verifiable architecture.

Every transmitted byte flows through open-source code — auditable, forkable, and independently verifiable

Deterministic payload generation enabling reproducible verification.



SemanticsAV Demo

Analyze malware samples instantly with AI-native detection

Enter SHA256 or MalwareBazaar URL

bd7644bfa1c8f6f195ed3d5c2a3ce8b3d69e8cf32d09176ec3ae626c5dcf72b6

Analyze

- Supported: PE (exe, dll), ELF
- Samples must be ≤7 days old

Examples:

`bd7644bfa1c8f6f195ed3d5c2a3ce8b3d69e8cf32d09176ec3ae626c5dcf72b6`

`https://bazaar.abuse.ch/sample/bd7644bfa1c8f6f195ed3d5c2a3ce8b3d69e8cf32d09176ec3ae626c5dcf72b6/`

Offline Scanner Performance

Configurations

	SemanticsAV	ClamAV
Engine Type	AI Model (Signatureless)	Signature-based
Engine Version	PE: 2025-10-28 05:18 UTC ELF: 2025-10-28 07:46 UTC	Latest version (2025-11-08): 8,724,498 total signatures

Malware Detection Test

- Dataset: MalwareBazaar daily bulk (2025.10.29 ~ 2025.11.05)
- PE: 701 / ELF: 1,056
- No custom labeling or filtering applied
- Original dataset used as-is for reproducibility
- MalwareBazaar may include benign files

False Positive Test

- Benign Sample Set
- 10,000 files from production systems
- Windows PE: 5,000 (random sampling)
- Linux ELF: 5,000 (random sampling)
- No false positives were detected in either SemanticsAV or ClamAV

Offline Scanner Performance

	SemanticsAV	ClamAV
Total Files Scanned	1,757	1,757
PE Detection Rate	91.58% (642/701)	15.26% (107/701)
ELF Detection Rate	99.24% (1,048/1,056)	75.57% (798/1,056)
Processing Time	37.2s	847.5s (14m 7s)
Throughput	99.5 MB/s	4.5 MB/s
Peak Memory	558 MB	1,782 MB
Average Memory	386 MB	1,496 MB

SemanticsAV Intelligence

① Verdict (Confidence)

SemanticsAV's detection verdict and confidence score

Confidence is identical to the offline scanner

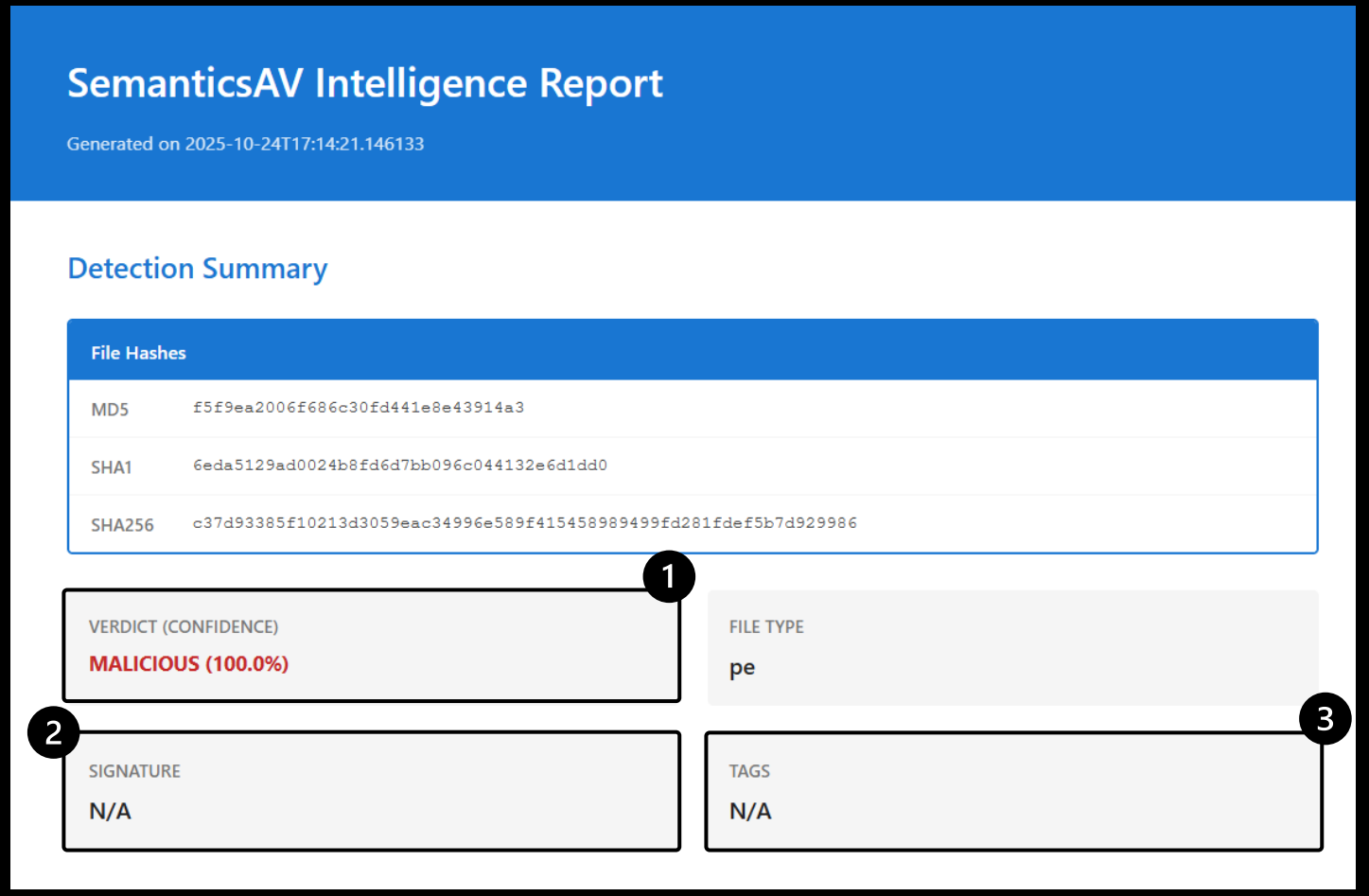
Detection threshold: 0.5

② ③ Signature & Tags

Malware Family Information

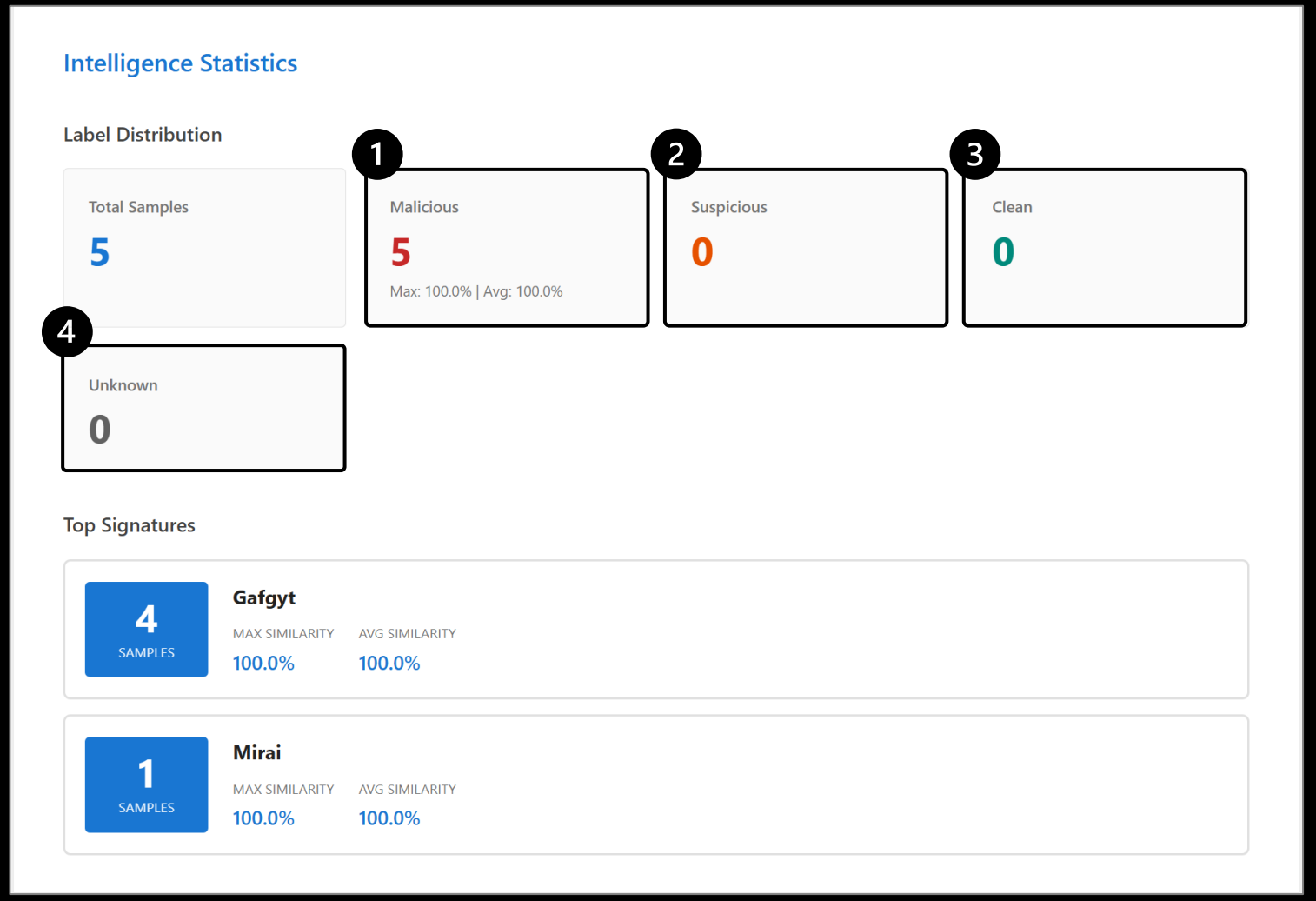
Signature and Tag values indicate an exact database match.

N/A indicates no matching sample exists (most common)



SemanticsAV Intelligence

1. **Malicious**
   Samples confirmed as malicious by the platform
2. **Suspicious**
   Samples collected from malware feeds but not yet confirmed as malicious
3. **Clean**
   Samples confirmed as benign by the platform
4. **Unknown**
   Samples collected from benign sources but not yet confirmed as benign



SemanticsAV Intelligence

Attribute Comparison Matrix

Compare static attributes between the target file and 5 similar samples from our threat intelligence database.

> Legend:
> † = Confirmed label (verified malicious/clean from intelligence)

1 2

Attribute	Target Baseline MALICIOUS† ■ Gafgyt elf Mirai upx-dec	Sample #1 100.0% MALICIOUS ■ Gafgyt 64 elf mirai	Sample #2 100.0% MALICIOUS ■ Gafgyt elf	Sample #3 100.0% MALICIOUS ■ Gafgyt 64 elf mirai	Sample #4 100.0% MALICIOUS ■ Gafgyt 64 elf mirai	Sample #5 100.0% MALICIOUS ■ Mirai 64 elf Gafgyt
build_id	N/A	N/A	N/A	N/A	N/A	N/A
class	64-bit	64-bit	64-bit	64-bit	64-bit	64-bit
compiler_info	N/A	N/A	N/A	N/A	N/A	N/A
▶ dynamic_entries.tags	[]	[]	[]	[]	[]	[]
dynamic_entries.total_count	0	0	0	0	0	0
endianness	Little	Little	Little	Little	Little	Little

3

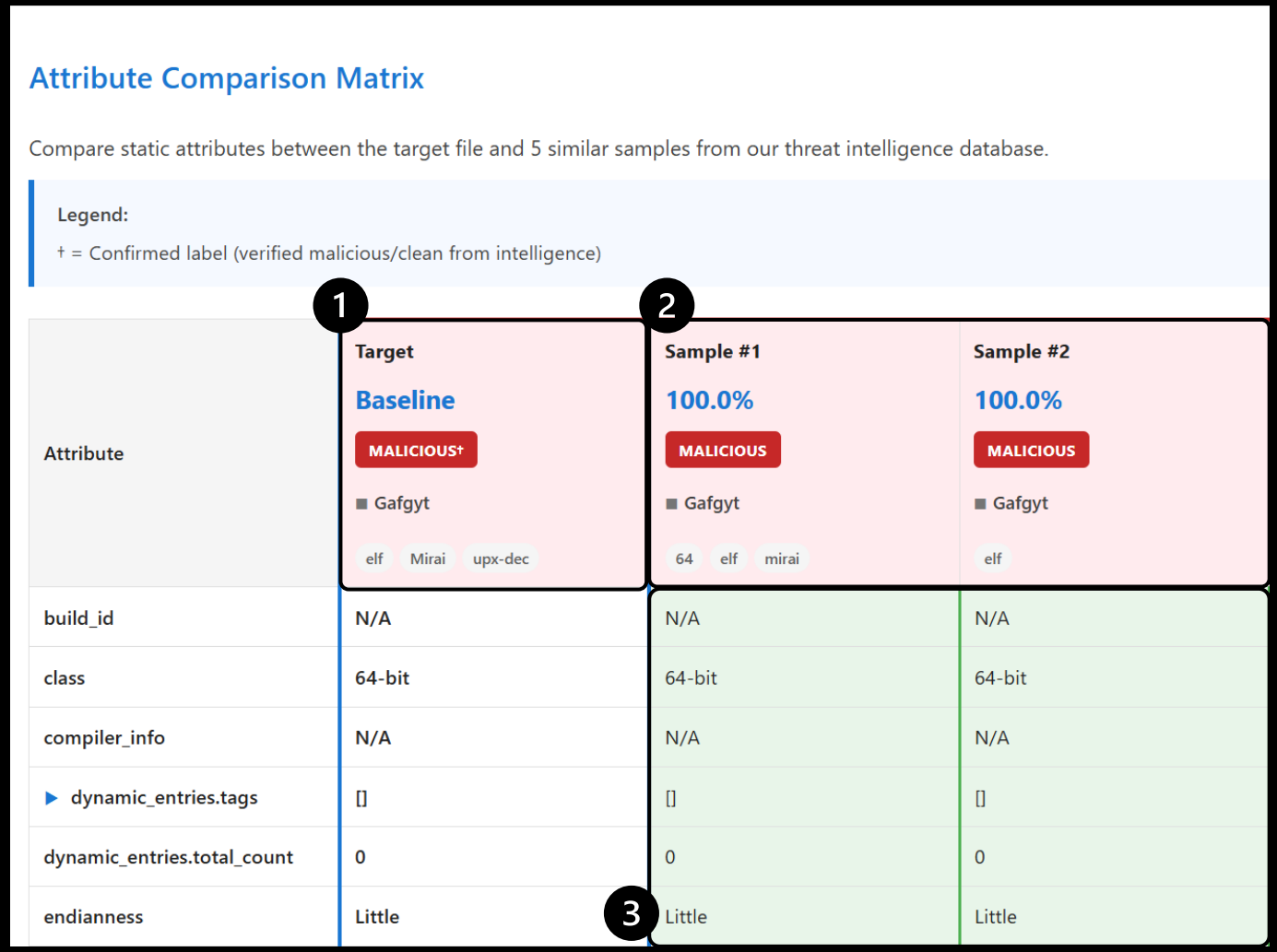
SemanticsAV Intelligence

① **Target Information**

② **Sample Information**

③ **Metadata**

Green: Aligned with Target
Yellow: Deviation from target



Attribute Comparison Matrix

Compare static attributes between the target file and 5 similar samples from our threat intelligence database.

Legend:

† = Confirmed label (verified malicious/clean from intelligence)

Attribute	Target Baseline MALICIOUS† ■ Gafgyt elf Mirai upx-dec	Sample #1 100.0% MALICIOUS ■ Gafgyt 64 elf mirai	Sample #2 100.0% MALICIOUS ■ Gafgyt elf
build_id	N/A	N/A	N/A
class	64-bit	64-bit	64-bit
compiler_info	N/A	N/A	N/A
▶ dynamic_entries.tags	[]	[]	[]
dynamic_entries.total_count	0	0	0
endianness	Little	Little	Little

SemanticsAV Intelligence

Verdict Summary

LLM-Powered Comprehensive Report Generation

- Technical Analysis
- Threat Intelligence Context
- Recommendations and Response Strategy

COPY REPORT

Executive Verdict Summary

The SemanticsAV Engine has identified this sample as MALICIOUS with 100.0% certainty. Structural analysis reveals a strong genetic link to known Gafgyt and Mirai malware families, indicating its likely use in IoT botnet operations and distributed denial-of-service (DDoS) attacks.

Technical Analysis

The target sample, an ELF executable, exhibits structural characteristics that firmly place it within the Gafgyt family. Analysis of its architectural patterns reveals a design intent focused on network scanning and exploitation, consistent with the typical behavior of this class of malware. Notably, the absence of imported libraries and a high number of exported symbols suggest a self-contained, purpose-built malicious agent designed for efficiency and evasion. Comparative analysis with similar samples in our intelligence database confirms a 100.0% geometric similarity, indicating a direct lineage and likely shared build environment or source code. The presence of the "upx-dec" tag further suggests a common obfuscation technique.

The specific internal structure, including the arrangement of sections and segments, aligns perfectly with known Gafgyt variants. This consistency points to a developer or group utilizing a standardized, potentially modular, codebase for their malicious toolkits. The lack of dynamic entries and the specific entry point further solidify this identification. These structural indicators are not merely superficial; they reflect the core design choices and functionalities embedded within the malware, pointing towards its role in reconnaissance and propagation within targeted networks, likely IoT devices.

Insights from SemanticsAV

1: Malware Ecosystem Discovery (1)

SemanticsAV discovered structural affinity across multiple malware families

Attribute	Target Baseline MALICIOUS† ■ a310Logger exe upx-dec	Sample #1 99.2% MALICIOUS ■ RemcosRAT exe RAT	Sample #2 99.2% MALICIOUS ■ a310Logger exe	Sample #3 99.2% MALICIOUS ■ RemcosRAT exe	Sample #4 99.2% MALICIOUS ■ RedLineStealer exe	Sample #5 99.2% MALICIOUS ■ DarkCloud exe
compilation_datetime	2025-11-04	2025-10-08	2025-07-22	2025-10-08	2025-07-31	2025-04-24
▶ data_directories.present	IMPORT_TABLE, RESOURCE_TABLE, BASE_RELOCATION_T..., ... (4 total)	IMPORT_TABLE, RESOURCE_TABLE, BASE_RELOCATION_T..., ... (6 total)	IMPORT_TABLE, RESOURCE_TABLE, BASE_RELOCATION_T..., ... (6 total)	IMPORT_TABLE, RESOURCE_TABLE, BASE_RELOCATION_T..., ... (6 total)	IMPORT_TABLE, RESOURCE_TABLE, BASE_RELOCATION_T..., ... (6 total)	IMPORT_TABLE, RESOURCE_TABLE, BASE_RELOCATION_T..., ... (6 total)
debug.by_type.RESERVED	N/A	1	1	1	1	1
debug.entries_count	0	1	1	1	1	1
delay_imports.dll_count	0	0	0	0	0	0

Family	Description
a310Logger	Crypto stealer & keylogger written in Visual Basic
RemcosRAT	Commercial Remote Access Trojan (RAT)
Redline Stealer	Popular Malware-as-a-Service (MaaS) infostealer
DarkCloud	Multi-stage Visual Basic stealer

Key Findings:

- One a310Logger sample mapped to 3 distinct malware families at 99.2% structural similarity.
- Validated via CTI reports (Avast Threat Labs (2021), ANOMALI Threat Research (2021), Rivista Cybersecurity Trends (2022)) showing these families share the same distribution environment and campaign.
- Ecosystem discovery achieved using static-only structural analysis → no signatures, no sandbox required.

Insights from SemanticsAV

1: Malware Ecosystem Discovery (2)

Static Structure Reveals Campaign-Level Linkages

Attribute	Target Baseline MALICIOUS†	Sample #1 99.8% MALICIOUS	Sample #2 99.8% MALICIOUS	Sample #3 99.8% MALICIOUS	Sample #4 99.8% SUSPICIOUS	Sample #5 99.8% MALICIOUS
	■ DeerStealer dropped-by-Amadey exe	■ RemcosRAT exe hijackloader rat remcos	■ DonutLoader exe	■ Arechclient2 5-10-250-239 exe GhostPulse HijackLoader SectopRAT ShadowLadder	■ AsyncRAT cachepeak-cfd exe	■ AZORult exe
compilation_datetime	2010-06-27	2010-06-27	2010-06-27	2010-06-27	2010-06-27	2010-06-27
version_info.file_type	APP	APP	APP	APP	APP	APP
version_info.file_version	1.4.0.1795	1.4.0.1795	1.4.0.1795	1.4.0.1795	1.4.0.1795	1.4.0.1795
version_info.product_version	1.4.0.1795	1.4.0.1795	1.4.0.1795	1.4.0.1795	1.4.0.1795	1.4.0.1795
version_info.strings.CompanyName	Oleg N. Scherbakov	Oleg N. Scherbakov	Oleg N. Scherbakov	Oleg N. Scherbakov	Oleg N. Scherbakov	Oleg N. Scherbakov
version_info.strings.FileDescription	7z Setup SFX (x86)	7z Setup SFX (x86)	7z Setup SFX (x86)	7z Setup SFX (x86)	7z Setup SFX (x86)	7z Setup SFX (x86)
version_info.strings.FileVersion	1.4.0.1795	1.4.0.1795	1.4.0.1795	1.4.0.1795	1.4.0.1795	1.4.0.1795
version_info.strings.InternalName	7ZSfxMod	7ZSfxMod	7ZSfxMod	7ZSfxMod	7ZSfxMod	7ZSfxMod
version_info.strings.LegalCopyright	Copyright © 2005-2010 Oleg N. Scherbakov	Copyright © 2005-2010 Oleg N. Scherbakov	Copyright © 2005-2010 Oleg N. Scherbakov	Copyright © 2005-2010 Oleg N. Scherbakov	Copyright © 2005-2010 Oleg N. Scherbakov	Copyright © 2005-2010 Oleg N. Scherbakov
version_info.strings.OriginalFilename	7ZSfxMod_x86.exe	7ZSfxMod_x86.exe	7ZSfxMod_x86.exe	7ZSfxMod_x86.exe	7ZSfxMod_x86.exe	7ZSfxMod_x86.exe
version_info.strings.PrivateBuild	June 27, 2010	June 27, 2010	June 27, 2010	June 27, 2010	June 27, 2010	June 27, 2010
version_info.strings.ProductName	7-Zip SFX	7-Zip SFX	7-Zip SFX	7-Zip SFX	7-Zip SFX	7-Zip SFX
version_info.strings.ProductVersion	1.4.0.1795	1.4.0.1795	1.4.0.1795	1.4.0.1795	1.4.0.1795	1.4.0.1795

Family	Description
DeerStealer	Subscription-based infostealer sold on dark-web forums
DonutLoader	Open-source in-memory shellcode loader
Arechclient2	Information stealer targeting credentials and system data
AsyncRAT	Open-source modular RAT
AZORult	Credential and cryptocurrency wallet stealer

Insights from SemanticsAV

1: Malware Ecosystem Discovery (2)

Static Structure Reveals Campaign-Level Linkages

Attribute	Target Baseline MALICIOUS† ■ DeerStealer dropped-by-Amadey exe	Sample #1 99.8% MALICIOUS ■ RemcosRAT exe hijackloader rat remcos	Sample #2 99.8% MALICIOUS ■ DonutLoader exe	Sample #3 99.8% MALICIOUS ■ Arechclient2 5-10-250-239 exe GhostPulse HijackLoader SectopRAT ShadowLadder	Sample #4 99.8% SUSPICIOUS ■ AsyncRAT cachepeak-cfd exe	Sample #5 99.8% MALICIOUS ■ AZORult exe
compilation_datetime	2010-06-27	2010-06-27	2010-06-27	2010-06-27	2010-06-27	2010-06-27
version_info.file_type	APP	APP	APP	APP	APP	APP
version_info.file_version	1.4.0.1795	1.4.0.1795	1.4.0.1795	1.4.0.1795	1.4.0.1795	1.4.0.1795
version_info.product_version	1.4.0.1795	1.4.0.1795	1.4.0.1795	1.4.0.1795	1.4.0.1795	1.4.0.1795
version_info.strings.CompanyName	Oleg N. Scherbakov	Oleg N. Scherbakov	Oleg N. Scherbakov	Oleg N. Scherbakov	Oleg N. Scherbakov	Oleg N. Scherbakov
version_info.strings.FileDescription	7z Setup SFX (x86)	7z Setup SFX (x86)	7z Setup SFX (x86)	7z Setup SFX (x86)	7z Setup SFX (x86)	7z Setup SFX (x86)
version_info.strings.FileVersion	1.4.0.1795	1.4.0.1795	1.4.0.1795	1.4.0.1795	1.4.0.1795	1.4.0.1795
version_info.strings.InternalName	7ZSfxMod	7ZSfxMod	7ZSfxMod	7ZSfxMod	7ZSfxMod	7ZSfxMod
	Copyright © 2005-2010 Oleg N.	Copyright © 2005-2010 Oleg N.	Copyright © 2005-2010 Oleg N.	Copyright © 2005-2010 Oleg N.	Copyright © 2005-2010 Oleg N.	Copyright © 2005-2010 Oleg N.

Malware Relationship	Evidence Type	Source
DeerStealer ↔ HijackLoader	Delivery Mechanism	Infosecurity Magazine (2025)
RemcosRAT ↔ DonutLoader	Campaign Infrastructure	Medium (2025)
HijackLoader ↔ Arechclient2	Payload Delivery	Red Canary (2025)
Amadey ↔ AZORult	Distribution Infrastructure	BlackBerry Cylance (2020)

Key Findings:

- SemanticsAV uncovered 5 distinct malware families sharing 99.8% architectural similarity.
- Identical 7z SFX build artifacts (2010-06-27 compile timestamp, v1.4.0.1795) across RemcosRAT, AsyncRAT, and multiple loaders indicate a shared MaaS production framework.
- Single-sample static analysis surfaced campaign-level relationships later confirmed by industry reporting (Amadey / HijackLoader distribution infrastructure).
- Rather than being limited to single-sample blocking, analysts can act on the underlying distribution supply chain.

Insights from SemanticsAV

1: Malware Ecosystem Discovery (3)

SemanticsAV reveals a common-build ecosystem between GhostSocks and SharkStealer

Attribute	Target Baseline MALICIOUS* 100.0% N/A	Sample #1 99.8% MALICIOUS GhostSocks exe signed	Sample #2 99.8% MALICIOUS SharkStealer exe signed	Sample #3 99.0% MALICIOUS SharkStealer dropped-by-ACRStealer exe signed	Sample #4 98.8% MALICIOUS SharkStealer dropped-by-ACRStealer exe signed	Sample #5 96.2% SUSPICIOUS GhostSocks dropped-by-ACRStealer exe signed
compilation_datetime	2025-07-08	2025-07-08	2025-07-08	2025-07-08	2025-07-08	2025-07-08
file_size	11926976	11961848	11926960	11927072	11926808	11961800
▸ signature.signers	CN=www.gga94ih3nb...	CN=www.tjvaq1vztq...	CN=www.syv9it0s0b...	CN=www.so72a3a478...	CN=www.a5scvo6i48...	CN=www.1g6z6kxqy3...
subsystem	WINDOWS_GUI	WINDOWS_GUI	WINDOWS_GUI	WINDOWS_GUI	WINDOWS_GUI	WINDOWS_GUI
symbols.total_count	0	0	0	0	0	0
tls.callbacks_count	0	0	0	0	0	0
tls.present	Yes	Yes	Yes	Yes	Yes	Yes
version_info.file_type	DLL	DLL	DLL	DLL	DLL	DLL
version_info.file_version	131.110.52845.41465	121.190.52862.58807	57.23.50140.16937	254.10.65534.0	200.50.40000.12340	100.200.30000.0
version_info.product_version	131.110.52845.41465	121.190.52862.58807	57.23.50140.16937	254.10.65534.0	200.50.40000.12340	100.200.30000.0
version_info.strings.						
version_info.strings.CompanyName	Flexera	Flexera	Flexera	Flexera	Flexera	Flexera
version_info.strings.FileDescription	Setup Suite Launcher Unicode	Setup Suite Launcher Unicode	Setup Suite Launcher Unicode	Setup Suite Launcher Unicode	Setup Suite Launcher Unicode	Setup Suite Launcher Unicode
version_info.strings.FileVersion	131.110.52845.41465	121.190.52862.58807	57.23.50140.16937	254.10.65534	200.50.40000.12340	100.200.30000
version_info.strings.ISInternalDescription	Setup Suite Launcher Unicode	Setup Suite Launcher Unicode	Setup Suite Launcher Unicode	Setup Suite Launcher Unicode	Setup Suite Launcher Unicode	Setup Suite Launcher Unicode
version_info.strings.ISInternalVersion	31.0.24	31.0.24	31.0.24	31.0.24	31.0.24	31.0.24
version_info.strings.Internal Build Number	215864	215864	215864	215864	215864	215864
version_info.strings.InternalName	SetupSuite	SetupSuite	SetupSuite	SetupSuite	SetupSuite	SetupSuite
version_info.strings.LegalCopyright	Copyright (c) 2025 Flexera. All Rights Reserved.	Copyright (c) 2025 Flexera. All Rights Reserved.	Copyright (c) 2025 Flexera. All Rights Reserved.	Copyright (c) 2025 Flexera. All Rights Reserved.	Copyright (c) 2025 Flexera. All Rights Reserved.	Copyright (c) 2025 Flexera. All Rights Reserved.
version_info.strings.OriginalFilename	клипт.exe	гост.exe	клипт.exe	clvJdvkJ2X2QzHLBdzN.exe	клипт.exe	socQ93HWkEQYPxz2fqdZ.exe
version_info.strings.ProductName	ft9bKpoqEX5atVwiAB	43oEYuPBjgb7i9RvbB	dQsyzotwgaCa87A2RG	A2rAoGkUzaKsVYWw8	WMNcndyvozTN2P	KpM3Ure2qoqNQaGsX
version_info.strings.ProductVersion	131.110.52845.41465	121.190.52862.58807	57.23.50140.16937	254.10.65534	200.50.40000.12340	100.200.30000

Family	Description
GhostSocks	Golang-based infostealer using blockchain-based EtherHiding exfiltrationxy (residential proxy node capability)
RemcosRAT	Golang-based infostealer using blockchain-based EtherHiding exfiltration

Insights from SemanticsAV

1: Malware Ecosystem Discovery (3)

SemanticsAV reveals a common-build ecosystem between GhostSocks and SharkStealer

Attribute	Target Baseline MALICIOUS* 100.0% N/A	Sample #1 99.8% MALICIOUS GhostSocks exe signed	Sample #2 99.8% MALICIOUS SharkStealer exe signed	Sample #3 99.0% MALICIOUS SharkStealer dropped-by-ACRStealer exe signed	Sample #4 98.8% MALICIOUS SharkStealer dropped-by-ACRStealer exe signed	Sample #5 96.2% SUSPICIOUS GhostSocks dropped-by-ACRStealer exe signed
compilation_datetime	2025-07-08	2025-07-08	2025-07-08	2025-07-08	2025-07-08	2025-07-08
file_size	11926976	11961848	11926960	11927072	11926808	11961800
version_info.strings.ISInternalVersion	31.0.24	31.0.24	31.0.24	31.0.24	31.0.24	31.0.24
version_info.strings.Internal Build Number	215864	215864	215864	215864	215864	215864
▶ signature.signers	CN=www.gga94ih3nb...	CN=www.tjvaq1vztq...	CN=www.syv9it0s0b...	CN=www.so72a3a478...	CN=www.a5scvo6i48...	CN=www.1g6z6kxqy3...
version_info.strings.ProductName	ft9bKpoqEX5atVwiAB	43oEYuPBjgb7i9RvbB	dQsyzotwgaCa87A2RG	A2rAoGkUzaKsVYWw8	WMNcndyvozTN2P	KpM3Ure2qoqNQaGsX

"To the best of our knowledge, no prior relationship between GhostSocks and SharkStealer has been documented in public threat intelligence."

Key Findings:

- Both GhostSocks and SharkStealer samples share identical compilation timestamp, proving simultaneous build from same infrastructure.
- All samples exhibit matching internal build parameters: ISInternalVersion, Build Number, identical CompanyName and FileDescription.
- Structural differences limited to randomized digital certificates and ProductName strings, classic polymorphic evasion technique.
- Implication: Our structural intelligence moves beyond validating known links to defining new malware ecosystems.

Insights from SemanticsAV

2 : Evolutionary Lineage Tracking (1)

Automatically revealing lineage, code reuse, and shared ancestry

Attribute	Target Baseline MALICIOUS† ■ Gunra exe ransomware	Sample #1 100.0% MALICIOUS ■ Gunra exe ransomware	Sample #2 96.5% MALICIOUS ■ Conti exe ransomware	Sample #3 96.2% MALICIOUS ■ Conti EAGLE Ransomware	Sample #4 96.2% MALICIOUS ■ Conti dll exe	Sample #5 96.1% MALICIOUS ■ Conti exe Ransomware
compilation_datetime	2025-04-15	2025-04-10	2021-04-16	2021-04-20	2021-04-20	2022-10-22
▸ data_directories.present	IMPORT_TABLE, RESOURCE_TABLE, EXCEPTION_TABLE, ... (7 total)	IMPORT_TABLE, RESOURCE_TABLE, EXCEPTION_TABLE, ... (7 total)	EXPORT_TABLE, IMPORT_TABLE, RESOURCE_TABLE, ... (8 total)	EXPORT_TABLE, IMPORT_TABLE, RESOURCE_TABLE, ... (8 total)	EXPORT_TABLE, IMPORT_TABLE, RESOURCE_TABLE, ... (8 total)	IMPORT_TABLE, RESOURCE_TABLE, EXCEPTION_TABLE, ... (7 total)
debug.by_type.ILTCG	1	1	1	1	1	1
debug.by_type.POGO	1	1	1	1	1	1
debug.entries_count	2	2	2	2	2	2
delay_imports.dll_count	0	0	0	0	0	0
delay_imports.total_functions	0	0	0	0	0	0
dll_characteristics.DYNAMIC_BASE	Yes	Yes	Yes	Yes	Yes	Yes
dll_characteristics.HIGH_ENTROPY_VA	Yes	Yes	Yes	Yes	Yes	Yes
dll_characteristics.NX_COMPAT	Yes	Yes	Yes	Yes	Yes	Yes

Conti: A Russia-based ransomware group (2020–2022) whose leaked internal code spawned multiple derivative variants.

Gunra: A new Apr-2025 ransomware built from leaked Conti's source code using double-extortion (Source: Gunra Ransomware: Conti-Derived Double-Extortion Threat Targeting Global Critical Sectors).

Key Findings:

- A single Gunra query mapped to four Conti variants, automatically validating the leaked codebase relationship.
- The system independently traced the evolutionary lineage from Conti (2021) to Gunra (2025).
- Demonstrates the ability to track malware evolution and code-reuse patterns.
- By exposing evolutionary links between attacks, malware genealogy enables proactive defense that anticipates the adversary's next move.

Insights from SemanticsAV

2 : Evolutionary Lineage Tracking (2)

Discovering undocumented ransomware relationships

Attribute	Target Baseline MALICIOUS† ■ BlackCat	Sample #1 96.7% MALICIOUS ■ BlackCat exe	Sample #2 90.5% MALICIOUS ■ RustyStealer Embargo exe Ransomware	Sample #3 84.5% MALICIOUS ■ RustyStealer exe	Sample #4 84.5% MALICIOUS ■ BlackCat exe Noberus ransomware	Sample #5 84.3% MALICIOUS ■ BlackCat BlackCat Indicators exe
compilation_datetime	2023-01-14	2023-02-28	2024-07-12	2007-02-10	2022-07-19	2022-06-01
▸ data_directories.present	IMPORT_TABLE, BASE_RELOCATION_T..., TLS_TABLE, ... (4 total)	IMPORT_TABLE, BASE_RELOCATION_T..., TLS_TABLE, ... (4 total)	IMPORT_TABLE, BASE_RELOCATION_T..., TLS_TABLE, ... (4 total)	IMPORT_TABLE, RESOURCE_TABLE, BASE_RELOCATION_T..., ... (5 total)	IMPORT_TABLE, BASE_RELOCATION_T..., TLS_TABLE, ... (4 total)	IMPORT_TABLE, BASE_RELOCATION_T..., TLS_TABLE, ... (4 total)
debug.entries_count	0	0	0	0	0	0
delay_imports.dll_count	0	0	0	0	0	0
delay_imports.total_functions	0	0	0	0	0	0
dll_characteristics.DYNAMIC_BASE	Yes	Yes	Yes	Yes	Yes	Yes
dll_characteristics.NX_COMPAT	Yes	Yes	Yes	Yes	Yes	Yes
entry_point	5296	5296	5280	5248	5296	5296
exports	N/A	N/A	N/A	N/A	N/A	N/A
file_size	7312384	7367680	6241792	1455104	3132416	3111424
image_size	7340032	7393280	6275072	1482752	3158016	3141632
▸ imports	[Array: 13 items]	[Array: 13 items]	[Array: 14 items]	[Array: 22 items]	[Array: 14 items]	[Array: 14 items]

BlackCat/ALPHV

- Rust-based ransomware-as-a-service (RaaS)
- First observed: Nov 2021
- Use double/triple extortion tactics globally

Embargo Ransomware (Known Relationship)

- Rust-based Raas group, emerged June 2024
- Targets: U.S. healthcare, business services, ..
- Assessed as BlackCat rebrand

(Source: Unmasking Embargo Ransomware: A Deep Dive Into the Group's TTPs and BlackCat Links 2025)

Insights from SemanticsAV

2 : Evolutionary Lineage Tracking (2)

Discovering undocumented ransomware relationships

Attribute	Target Baseline MALICIOUS† ■ BlackCat	Sample #1 96.7% MALICIOUS ■ BlackCat exe	Sample #2 90.5% MALICIOUS ■ RustyStealer Embargo exe Ransomware	Sample #3 84.5% MALICIOUS ■ RustyStealer exe	Sample #4 84.5% MALICIOUS ■ BlackCat exe Noberus ransomware	Sample #5 84.3% MALICIOUS ■ BlackCat BlackCat Indicators exe
compilation_datetime	2023-01-14	2023-02-28	2024-07-12	2007-02-10	2022-07-19	2022-06-01
▸ data_directories.present	IMPORT_TABLE, BASE_RELOCATION_T..., TLS_TABLE, ... (4 total)	IMPORT_TABLE, BASE_RELOCATION_T..., TLS_TABLE, ... (4 total)	IMPORT_TABLE, BASE_RELOCATION_T..., TLS_TABLE, ... (4 total)	IMPORT_TABLE, RESOURCE_TABLE, BASE_RELOCATION_T..., ... (5 total)	IMPORT_TABLE, BASE_RELOCATION_T..., TLS_TABLE, ... (4 total)	IMPORT_TABLE, BASE_RELOCATION_T..., TLS_TABLE, ... (4 total)
debug.entries_count	0	0	0	0	0	0
delay_imports.dll_count	0	0	0	0	0	0

RustyStealer (Undocumented Relationship)

- Rust-compiled information stealer
- Exfiltrates data from browsers, email clients, crypto wallets, password managers
- No publicly documented connection to BalckCat

Key Findings:

- Existing threat intelligence has suggested Embargo-BlackCat relationships through operational similarities.
- Compilation timestamps (BlackCat: Jan 2023 → Embargo: Jul 2024) align with BlackCat's disruption timeline, supporting the strategic rebrand hypothesis.
- SemanticsAV detected 90.5% architectural similarity between the target BlackCat sample and a file tagged as both RustyStealer and Embargo, revealing a previously undocumented connection.
- The triangular relationship (RustyStealer ↔ Embargo ↔ BlackCat) suggests shared development infrastructure or coordinated operations rather than coincidental overlap.

Insights from SemanticsAV

3: Polymorphism as Fingerprint

Stealc Campaign — Evasion Through Polymorphic Identities

Attribute	Target Baseline MALICIOUS† ■ Stealc exe	Sample #1 98.5% MALICIOUS ■ Stealc exe	Sample #2 98.2% MALICIOUS ■ Stealc exe	Sample #3 98.1% MALICIOUS ■ Stealc exe	Sample #4 97.9% MALICIOUS ■ Stealc exe	Sample #5 97.3% MALICIOUS ■ Stealc exe
compilation_datetime	2025-10-12	2025-10-12	2025-10-12	2025-10-12	2025-10-12	2025-10-12
▸ data_directories.present	IMPORT_TABLE, RESOURCE_TABLE, EXCEPTION_TABLE, ... (6 total)	IMPORT_TABLE, RESOURCE_TABLE, EXCEPTION_TABLE, ... (6 total)	IMPORT_TABLE, RESOURCE_TABLE, EXCEPTION_TABLE, ... (6 total)	IMPORT_TABLE, RESOURCE_TABLE, EXCEPTION_TABLE, ... (6 total)	IMPORT_TABLE, RESOURCE_TABLE, EXCEPTION_TABLE, ... (6 total)	IMPORT_TABLE, RESOURCE_TABLE, EXCEPTION_TABLE, ... (6 total)
entry_point	6365272	6557784	6357080	6357080	6148184	6148184
exports	N/A	N/A	N/A	N/A	N/A	N/A
file_size	3624384	3742144	3607488	3590080	3306432	3387328
image_size	9437184	9760768	9424896	9404416	8916992	8998912
▸ imports	[Array: 1 items]	[Array: 1 items]	[Array: 1 items]	[Array: 1 items]	[Array: 1 items]	[Array: 1 items]
▾ sections	, , , ... (11 total)	, , , ... (11 total)	, , , ... (11 total)	, , , ... (11 total)	, , , ... (11 total)	, , , ... (11 total)

Target	Sample #1 (98.5%)	Sample #2 (98.2%)	Sample #3 (98.1%)	Sample #4 (97.9%)	Sample #5 (97.3%)
[".rsrc", ".idata", ".tls", ".themida", ".boot", ".reloc"]	[".rsrc", ".idata", ".tls", ".themida", ".boot", ".reloc"]	[".rsrc", ".idata", ".tls", ".themida", ".boot", ".reloc"]	[".rsrc", ".idata", ".tls", ".themida", ".boot", ".reloc"]	[".rsrc", ".idata", ".tls", ".themida", ".boot", ".reloc"]	[".rsrc", ".idata", ".tls", ".themida", ".boot", ".reloc"]

Attribute	Target	Sample #1	Sample #2	Sample #3	Sample #4	Sample #5
version_info.file_version	1.0.46.420	3.1.66.65	3.5.23.139	2.8.24.330	5.4.85.771	4.3.59.733
version_info.product_version	1.0.46.420	3.1.66.65	3.5.23.139	2.8.24.330	5.4.85.771	4.3.59.733
version_info.strings.CompanyName	Simutronics Corporation	Quantum Dynamics	BrightWave Software	Fusion Labs	Orion Dynamics	Elite Software
version_info.strings.FileDescription	Titan Solution Platform	Nebula Solution Framework	Unity Creative Toolkit	Echo Management Platform	Horizon Creative Framework	Unity Creative Toolkit
version_info.strings.FileVersion	1.0.46	3.1.66	3.5.23	2.8.24	5.4.85	4.3.59
version_info.strings.InternalName	nebulaplatform	nebulaplatform	quantum	genesisengine	horizonsuite	fusionengine
version_info.strings.LegalCopyright	© 2020 Simutronics Corporation.	© 2025 Quantum Dynamics.	© 2004 BrightWave Software.	© 2005 Fusion Labs.	© 2022 Orion Dynamics.	© 2012 Elite Software.
version_info.strings.OriginalFilename	fusionengine.exe	pinnaclestudio.exe	elitebuilder.exe	pinnaclestudio.exe	orionsuite.exe	nexus.exe
version_info.strings.ProductName	Nebula Platform	Horizon Suite	Fusion Engine	Titan IDE	HeroEngine	Elite Builder
version_info.strings.ProductVersion	1.0.46	3.1.66	3.5.23	2.8.24	5.4.85	4.3.59

Overview

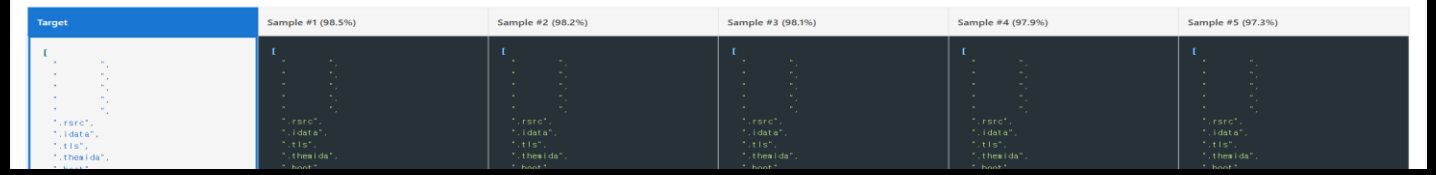
- Stealc: information-stealing malware targeting browser credentials and crypto wallets
- Themida protection: commercial packer; heavy encryption and anti-analysis make static analysis impractical.
- Polymorphic metadata: per-sample CompanyName / ProductName changes to evade reputation-based detection.

Insights from SemanticsAV

3: Polymorphism as Fingerprint

Stealc Campaign — Evasion Through Polymorphic Identities

Attribute	Target Baseline MALICIOUS Stealc	Sample #1 98.5% MALICIOUS Stealc	Sample #2 98.2% MALICIOUS Stealc	Sample #3 98.1% MALICIOUS Stealc	Sample #4 97.9% MALICIOUS Stealc	Sample #5 97.3% MALICIOUS Stealc
compilation_datetime	2025-10-12	2025-10-12	2025-10-12	2025-10-12	2025-10-12	2025-10-12
▸ data_directories.present	IMPORT_TABLE, RESOURCE_TABLE, EXCEPTION_TABLE, ... (6 total)	IMPORT_TABLE, RESOURCE_TABLE, EXCEPTION_TABLE, ... (6 total)	IMPORT_TABLE, RESOURCE_TABLE, EXCEPTION_TABLE, ... (6 total)	IMPORT_TABLE, RESOURCE_TABLE, EXCEPTION_TABLE, ... (6 total)	IMPORT_TABLE, RESOURCE_TABLE, EXCEPTION_TABLE, ... (6 total)	IMPORT_TABLE, RESOURCE_TABLE, EXCEPTION_TABLE, ... (6 total)
entry_point	6365272	6557784	6357080	6357080	6148184	6148184
exports	N/A	N/A	N/A	N/A	N/A	N/A
file_size	3624384	3742144	3607488	3590080	3306432	3387328
image_size	9437184	9760768	9424896	9404416	8916992	8998912
▸ imports	[Array: 1 items]	[Array: 1 items]	[Array: 1 items]	[Array: 1 items]	[Array: 1 items]	[Array: 1 items]
▾ sections	, , , ... (11 total)	, , , ... (11 total)	, , , ... (11 total)	, , , ... (11 total)	, , , ... (11 total)	, , , ... (11 total)



"Even when packed with commercial packers such as Themida, SemanticsAV's static analysis can still identify the malware campaign."

Key Findings:

- Attackers easily neutralize traditional defenses by combining commercial packers with trivial metadata tweaks.
- SemanticsAV treats these evasion techniques as persistent structural fingerprints rather than obstacles.
- This undermines the attacker's low-cost repackaging model and forces re-engineering of core malware architecture — increasing attacker cost and complexity.

The Paradigm Inverts

01

Evasion Becomes Evidence.

Obfuscation no longer hides malware
SemanticsAV turns evasion into a structural signal

02

Defenders Automate. Attackers Can’t.

Defenders generalize from every new sample
Attackers must manually redesign architectures
→ Automation asymmetry becomes defensive leverage

03

Reuse Dies. Economics Invert.

Architectural reuse fails under semantic detection
→ Attackers must pay full development cost for every variant

Q&A