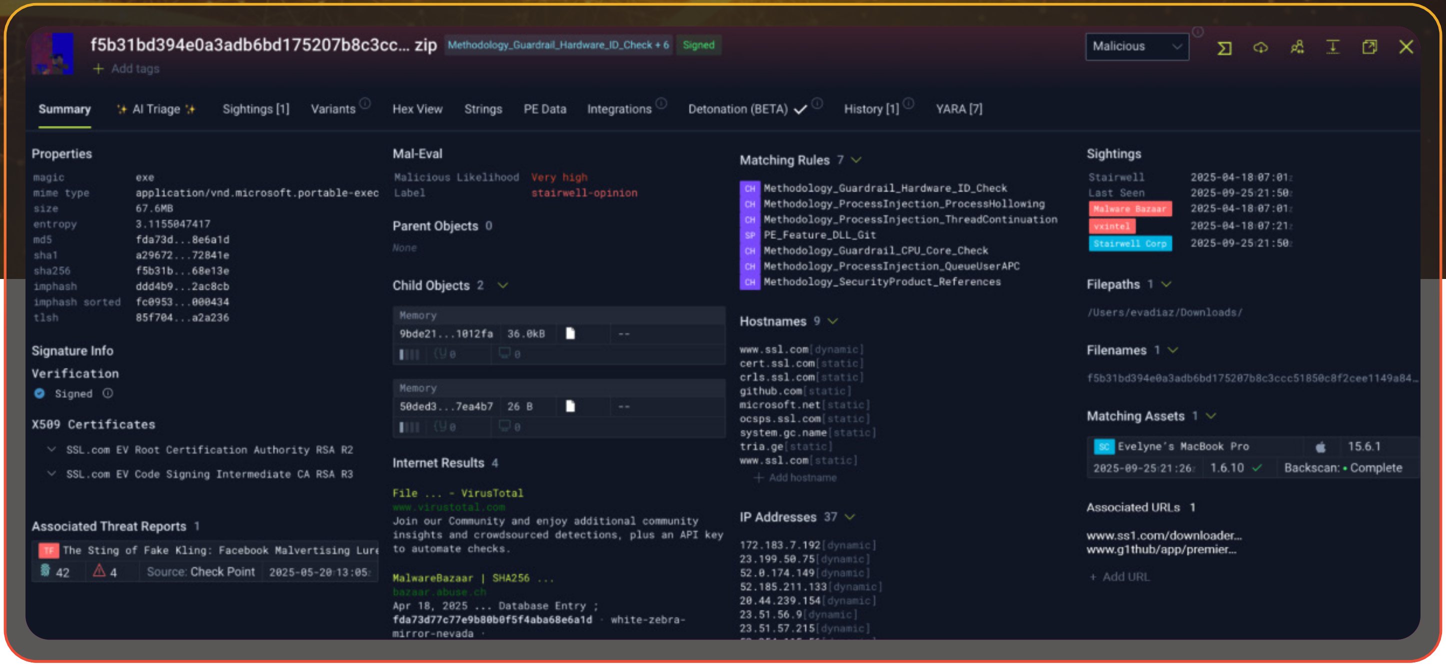
CONTINUOUS ANALYSIS OF EVERYTHING. IN YOUR OWN PRIVATE VAULT.

Deep intelligence across files, URLs, domains, IPs, and DNS. Privately and continuously.



f5b31bd394e0a3adb6bd175207b8c3cc... zip Methodology_Guardrail_Hardware_ID_Check + 6 Signed

Properties

magic	exe
mime type	application/vnd.microsoft.portable-exec
size	67.6MB
entropy	3.1155047417
md5	fda73d...8e6a1d
sha1	a29672...72841e
sha256	f5b31b...68e13e
imphash	ddd4b9...2ac8cb
imphash sorted	fc0953...000434
tlsh	85f704...a2a236

Signature Info

Verification

Signed

X509 Certificates

SSL.com EV Root Certification Authority RSA R2

SSL.com EV Code Signing Intermediate CA RSA R3

Associated Threat Reports 1

TF The Sting of Fake Kling: Facebook Malvertising Lure
42 | 4 | Source: Check Point | 2025-05-20 13:05

Mal-Eval

Malicious Likelihood	Very high
Label	stairwell-opinion

Parent Objects 0

None

Child Objects 2

Memory			
9bde21...1012fa	36.0kB		--
	0	0	

Memory			
50ded3...7ea4b7	26 B		--
	0	0	

Internet Results 4

File ... - VirusTotal
www.virustotal.com
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

MalwareBazaar | SHA256 ...
bazaar.abuse.ch
Apr 18, 2025 ... Database Entry ; fda73d77c77e9b80b0f5f4aba68e6a1d · white-zebra-mirror-nevada ·

Matching Rules 7

- CH Methodology_Guardrail_Hardware_ID_Check
- CH Methodology_ProcessInjection_ProcessHollowing
- CH Methodology_ProcessInjection_ThreadContinuation
- SP PE_Feature_DLL_Git
- CH Methodology_Guardrail_CPU_Core_Check
- CH Methodology_ProcessInjection_QueueUserAPC
- CH Methodology_SecurityProduct_References

Hostnames 9

www.ssl.com[dynamic]
cert.ssl.com[static]
crls.ssl.com[static]
github.com[static]
microsoft.net[static]
ocsps.ssl.com[static]
system.gc.name[static]
tria.ge[static]
www.ssl.com[static]

IP Addresses 37

172.183.7.192[dynamic]
23.199.50.75[dynamic]
52.0.174.149[dynamic]
52.185.211.133[dynamic]
20.44.239.154[dynamic]
23.51.56.9[dynamic]
23.51.57.215[dynamic]

Sightings

Stairwell	2025-04-18 07:01
Last Seen	2025-09-25 21:50
Malware Bazaar	2025-04-18 07:01
vxintel	2025-04-18 07:21
Stairwell Corp	2025-09-25 21:50

Filepaths 1

/Users/evadiaz/Downloads/

Filenames 1

f5b31bd394e0a3adb6bd175207b8c3ccc51850c8f2cee1149a84...

Matching Assets 1

SC Evelyne's MacBook Pro		15.6.1
2025-09-25 21:26	1.6.10 ✓	Backscan: • Complete

Associated URLs 1

www.ss1.com/downloader...
www.g1thub/app/premier...

THE LIMITATIONS OF TRADITIONAL FILE ANALYSIS TOOLS

The main weakness of crowdsourced 'file analysis' tools is the lack of privacy because everyone gets access to your uploaded files. Also, many solutions are built around a single artifact type, forcing defenders to jump between tools for URLs, domains, IPs, or related infrastructure. Enterprises depend on file analysis platforms to identify and understand potential threats, but traditional solutions come with serious trade-offs.

PRIVACY CONCERNS

Many analysis platforms rely on shared or public scanning infrastructure, risking exposure of sensitive data and intellectual property to outside entities, including potential adversarial nations.

VERDICT CONFUSION

These tools often deliver shallow, signature-based results that lack context for emerging or targeted threats. Inconsistent verdicts across multiple, legacy antivirus engines only add to the uncertainty.

POINT-IN-TIME VISIBILITY

Threat intelligence changes daily. But most platforms only analyze an object on upload. Hindsight, context, and historical knowledge are lost.

BUDGET COMPROMISES

Budget and usage limits frequently force security teams to scale back using key features, or hoard their quota today in case it's needed tomorrow, reducing overall effectiveness and visibility.

CONTINUOUS ANALYSIS OF EVERYTHING. IN YOUR OWN PRIVATE VAULT.

As adversaries grow more sophisticated, security teams need a private, context-rich alternative that preserves data confidentiality, accelerates investigations, and integrates seamlessly into existing detection and response workflows.

WHAT IS STAIRWELL?

Stairwell is a private, continuous intelligence system that ingests and connects every object tied to an attack: executables, scripts, URLs, IPs, domains, and DNS history, into a complete, queryable picture. Unlike VirusTotal, where uploaded data leaks to the world, Stairwell provides your own private vault. You get over a billion malware samples spanning 5+ years, plus the ability to run deep, historical analysis, in your environment, without tipping off an adversary.

KEY FEATURES

FILE LOOKUPS	Instant context on files, URLs, domains, IPs, and DNS history, all enriched with verdicts, prevalence, metadata, strings, entropy, YARA matches, and more.
PRIVATE VAULT	Your data stays private. Every artifact is stored securely and never shared outside your enterprise.
AI TRIAGE	Reverse engineer–level analysis of executables and scripts to reveal what the file does and why it matters.
YARA HUNTS	Write once, run forever. YARA rules scan all artifact types across all historical data, no manual re-runs needed. No 90, 180, or 365 day limitations on visibility.
VARIANT DISCOVERY	Automatically identify repacked, polymorphic, and lineage-related files across your vault and global corpus, over time.
THREAT INTEL CORRELATION	Full-spectrum correlation of IOCs, YARA, DNS history, and global + local sightings.

10 REASONS SECURITY TEAMS SWITCH TO STAIRWELL

1. **PRIVATE VAULT FOR ALL ARTIFACTS**
Your files, artifacts, URLs, IPs, and DNS relationships are stored in your own private vault, never shared, never leaked.

2. **CONTINUOUS ANALYSIS**
Unlike other solutions where analysis is point-in-time, Stairwell stores and reanalyzes files and artifacts perpetually, with no 90-day cutoff or loss of history.

3. **ENTERPRISE-WIDE HINDSIGHT**
Know if any file, domain, IP, or URL has ever touched any system across your environment.

4. **ONE CLEAR VERDICT**
Get a definitive assessment enriched with global threat intelligence, variant relationships, and historical prevalence.

5. **AI MALWARE ANALYSIS**
Skip the sandboxes and signatures. Instantly understand what a file does, how it behaves, and whether it's a threat. Detonation evasion becomes a lost art.

6. **UPSKILL YOUR ANALYSTS WITH EXPERT-LEVEL INSIGHT**
Analyzes what a file does, not just what it looks like. Instantly understand intent, behavior, and risk so your SOC team can make confident decisions without wasting time on manual reversing or waiting on dynamic analysis.

7. **HIDDEN MALWARE VARIANT DETECTION**
See beyond hashes. Map malware families, uncover polymorphic variants, and trace campaigns across both your environment and our 1PB+ global corpus.

8. **CONTINUOUS YARA**
Run YARA rules at planet scale. Manage and write your own rules. Run them live and retro at scale.

9. **REDUCED SANDBOX USAGE**
Analyzing files using AI Triage results in fewer sandbox detonations and measurable cost savings for file analysis needs.

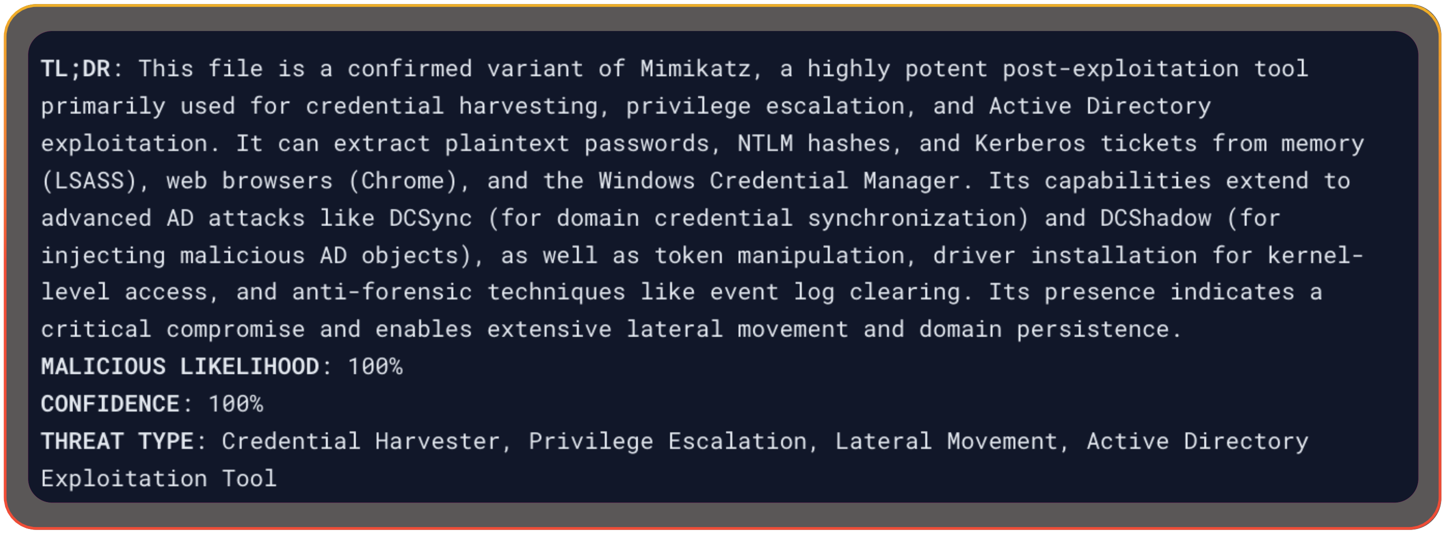
10. **COST EFFECTIVE PRICING**
Flat access pricing includes YARA searches with no 'retro hunt' fees, unlimited recursive variant discovery, and file retention – without the enterprise price tag.

CONTINUOUS ANALYSIS OF EVERYTHING. IN YOUR OWN PRIVATE VAULT.

MALWARE EVADES TOOLS. IT CAN'T HIDE FROM THE TRUTH.

Most detection tools watch what malware does, but attackers know that. If malware sees it's running in a sandbox or on a researcher's machine, it simply shuts off or changes behavior. That's how easy it is to slip past traditional defenses.

It's time to step outside the sandbox. AI Triage reads the file itself. It uses advanced AI and deep threat intelligence to explain exactly what the file is designed to do, no matter how it behaves at runtime. Avoids evasion and delivers clear, trusted analysis you can act on.



```
TL;DR: This file is a confirmed variant of Mimikatz, a highly potent post-exploitation tool
primarily used for credential harvesting, privilege escalation, and Active Directory
exploitation. It can extract plaintext passwords, NTLM hashes, and Kerberos tickets from memory
(LSASS), web browsers (Chrome), and the Windows Credential Manager. Its capabilities extend to
advanced AD attacks like DCSync (for domain credential synchronization) and DCShadow (for
injecting malicious AD objects), as well as token manipulation, driver installation for kernel-
level access, and anti-forensic techniques like event log clearing. Its presence indicates a
critical compromise and enables extensive lateral movement and domain persistence.
MALICIOUS LIKELIHOOD: 100%
CONFIDENCE: 100%
THREAT TYPE: Credential Harvester, Privilege Escalation, Lateral Movement, Active Directory
Exploitation Tool
```

STAIRWELL INTELLIGENCE GOES BEYOND THE FILE.

Stairwell doesn't just scan files, it understands your entire threat surface. Files, URLs, Domains, IPs, and DNS history are all preserved, analyzed, and connected in one system built for deep, continuous intelligence.

Where other solutions show you what the crowd has seen recently. Stairwell privately shows you what actually matters — the maliciousness of every file, the full history of every file, with unlimited search, YARA, variant discovery and the infrastructure behind every artifact. This is intelligence, not just 'file scanning'.

CONTINUOUS ANALYSIS OF EVERYTHING. IN YOUR OWN PRIVATE VAULT.

STAIRWELL.COM/REQUEST-A-DEMO/

STAIRWELL