RATS Working Group
Internet-Draft
Intended status: Informational
Expires: 5 December 2026

L. Melegassi
Catellix

3 June 2026

MVPS-Memory: Multi-Vantage Coherence Detection of Memory-Resident Malware, Anchored in Remote Attestation

draft-melegassi-rats-mvps-memory-coherence-00

Abstract

Memory-resident ("fileless", in-memory) malware -- reflective code injection, page-cache .text patching, process hollowing, RX->RWX permission flips, unbacked-memory thread starts, token theft, and patchless AMSI/ETW suppression -- leaves the on-disk image unchanged and is therefore structurally invisible to signature and file-integrity detectors. This document explains why, and what removes the blind spot, using the Multi-Vantage Path Synchrony (MVPS) observability model y = H x: each detection facility is a row (a projection) of one observation operator H over an interior runtime-memory state x, and a purely in-memory implant is an attack whose damage direction c lies in the NULL SPACE of any single on-disk vantage.

The contribution uses no new mathematics. It (1) instantiates the already-proved MVPS results -- the Stealth-Manifold Lemma, the coordination-stealth duality, the Stealth Conservation Law max(0, k - rho), the reflexive tower, the data-processing ceiling, the non-blinding invariant (stealth + effect = ||a||^2), and the silent-effect ceiling (E < tau^2) -- verbatim on the runtime-memory surface; (2) anchors the meta-observer in the RATS architecture [RFC9334], whose Attester is defined to collect Claims by "taking measurements on code, memory, or other security related assets", with TPM-based Remote Integrity Verification [RFC9683], the Entity Attestation Token [RFC9711], the Concise Reference Integrity Manifest [I-D.ietf-rats-corim], and Concise Software Identification [RFC9393] as the evidence/reference-value layer; and (3) closes the vantage-forgery channel with post-quantum eye identity (ML-DSA, FIPS 204, via [I-D.ietf-cose-dilithium] and [I-D.ietf-lamps-dilithium-certificates]). A live threat anchor -- the 2025-2026 surge in BYOVD EDR-killers (e.g. CVE-2025-68947) and patchless AMSI/ETW suppression -- is shown to be a textbook instance of the eye-silencing law. All theorem-level claims carry a machine-checkable numerical receipt.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

A signature or file-integrity detector learns or hashes the bytes a program has ON DISK and alarms on deviation. A memory-resident implant never changes those bytes: it acts entirely in the live address space -- patching the in-memory copy of .text in the page cache, flipping a region from read-execute to read-write-execute, starting a thread at private/unbacked executable memory, stealing a token, or suppressing AMSI/ETW so the very telemetry that would report it goes quiet. Against an on-disk vantage this is not "hard to see"; it is structurally INVISIBLE.

The Multi-Vantage Path Synchrony (MVPS) framework models a set of detection facilities as rows of one observation operator H acting on an interior state x, producing observations y = H x; an attack is a damage direction c with effect d = c^T x. In that model the claim of this document is exact: a purely in-memory implant is a c that lies in null(H) of any single on-disk vantage, and the remedy is not a cleverer classifier but ADDING vantages whose joint rowspace covers c -- "spend probes, not parameters".

This is the same observability spine already applied to the Linux kernel surface [I-D.melegassi-opsawg-mvps-os-host]; here it is applied to runtime memory and, critically, the meta-observer that watches for silenced eyes is identified with the RATS architecture [RFC9334]. RFC 9334 defines an Attester that collects Claims by

"reading system registers and variables, calling into subsystems, taking measurements on code, memory, or other security related assets of the Target Environment"; remote attestation of memory state is therefore already in scope of a standardised architecture, with

TPM-based Remote Integrity Verification [RFC9683] and the Entity Attestation Token [RFC9711] supplying the evidence layer and the Concise Reference Integrity Manifest [I-D.ietf-rats-corim] / Concise Software Identification [RFC9393] supplying Reference Values.

Claims are made at three maturity levels per the MVPS adversarial-audit methodology [I-D.melegassi-irtf-mvps-methodology]: [T] machine-checked theorems, [D] engineering designs, and [C] conjectures with falsification protocols. Every [T] claim here is exercised by scripts/validate_memory_coherence.py (Section 13).

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

Eye (vantage): one detection facility, a row of H, observing a projection of the runtime-memory state x (e.g. an in-memory code scanner, a VM-permission monitor, an ETW thread provider, a PMU counter, a TPM PCR).

Damage direction c: the direction in state space that an attack perturbs; d = c^T x is its effect. null(H) is the set of c that no attached eye observes.

Memory-resident implant: malware whose damage direction has zero component on the on-disk coordinate(s); a.k.a. fileless / in-memory.

Eye redundancy rho: rho = m - n for an H with m independent eyes over an n-dimensional state; the overlap that absorbs silenced eyes.

The MVPS terms Stealth-Manifold Lemma, coordination-stealth duality (T-CSD), Stealth Conservation Law, reflexive tower, data-processing ceiling, non-blinding invariant, and silent-effect ceiling are used as defined in [I-D.melegassi-irtf-mvps-methodology] and its companions.

3. Threat Anchor: BYOVD EDR-Killers and Patchless AMSI/ETW

The eye-silencing law of Section 8 is not hypothetical; it is the dominant real-world defence-evasion technique. Public reporting in 2025-2026 describes:

o Bring Your Own Vulnerable Driver (BYOVD): a campaign loads a legitimately SIGNED but vulnerable kernel driver, then exploits it from user space to gain kernel execution and TERMINATE EDR/AV processes, unregister kernel callbacks (process/thread/image-load), and wipe telemetry before the main payload runs. CVE-2025-68947 (NSecKrnl.sys, abused by the Reynolds ransomware, which bundles the driver in the payload) is one instance; a March 2026 analysis counted

54 distinct EDR-killers abusing 35 signed drivers. The Qilin EDR-killer can terminate 300+ EDR drivers and runs its loader entirely in memory.

o Patchless AMSI/ETW suppression: Vectored Exception Handling and hardware breakpoints intercept and spoof scan results WITHOUT modifying in-memory code, silencing the scanning eye while leaving no .text patch.

Two facts make this a textbook MVPS case:

(a) The implant body and the EDR-killer loader are MEMORY-RESIDENT (MITRE ATT&CK T1055 Process Injection); the on-disk artefact is a signed, trusted driver. A signature/file-integrity vantage has the damage direction in its null space (T-MEM-1). The decisive move is

then to silence the eyes (ATT&CK T1562.001 Impair Defenses; T1014 Rootkit) -- exactly the Stealth Conservation Law (T-MEM-4): k callbacks/providers silenced re-open max(0, k - rho) blind dimensions.

(b) Crucially, attackers do NOT forge the driver’s signature; they REUSE a valid one on a vulnerable driver (ATT&CK T1068). In MVPS terms the forgery channel is closed and the residual attack is the GEOMETRIC eye-silencing one (Section 11, T-MEM-7) -- which is precisely the channel a reflexive, attested meta-observer flags (T-MEM-5). This real-world fact corroborates the non-blinding split: defenders should spend their cryptographic budget on authenticated eye identity and their telemetry budget on redundant, diverse eyes, not on out-computing the attacker.

The operator takeaway echoed in that reporting -- "EDR alone is no longer sufficient; layer kernel driver-load monitoring, immutable logging, and attestation" -- is the MVPS prescription stated informally: raise rho, add the driver-load eye, and terminate the tower in an attested root of trust.

4. The Object: Runtime Memory as a Vantage Stack

Let x in R^n be the interior runtime-memory state of a host over one observation tick. The receipt uses n = 12 named coordinates, including on-disk image bytes, in-memory .text patch (page-cache writeback), RX->RWX permission flip, unbacked-memory exec thread,

token/UID-0 transition, AMSI/ETW userland patch, per-region allocation, direct (unhooked) syscall, reflective module load, network C2 beacon, and the TPM PCR / measured-boot value. Each detection facility is a row of H observing the coordinates it can measure; y = H x is the union of what the attached eyes report.

Every MVPS observability result holds on this surface without re-proof, because it is the same linear map. Sections 5-11 state the eight that bear on memory-resident malware.

5. Why a Single On-Disk Vantage Cannot See It (T-MEM-1)

T-MEM-1 [T] (fileless blind subspace). For an on-disk-image-only operator H_disk and a memory-resident implant direction c with zero on-disk component, H_disk c = 0 and the entire damage lies in

null(H_disk): the implant is invisible to that vantage yet damaging. This is the Stealth-Manifold Lemma instantiated on memory.

Receipt witness: |H_disk c| = 0, |P_null c| = 1.715 (all damage hidden), on-disk component 0 by construction.

CONSEQUENCE. No improvement to a signature engine -- larger hash

sets, more rules, a bigger model -- can recover a direction its rows do not span (see T-MEM-6). The deficiency is geometric, not computational.

6. Coherent Cover Closes It (T-MEM-2)

T-MEM-2 [T] (coherent cover). Adding runtime memory eyes in correlation order -- in-memory .text scan (page cache), VM-permission monitor, unbacked-thread provider, token/credential hook -- removes one dimension of attacker freedom at a time: the hideable fraction eta = dim(null H)/n is monotone non-increasing and the undetected-damage value ||P_null c||^2 falls to 0 once the eye-set covers c.

Receipt witness (eyes added 1..5):

eyes:	1(disk)	2(+pgc)	3(+vm)	4(+thr)	5(+tok)
eta :	0.9167	0.8333	0.7500	0.6667	0.5833
value:	2.94	1.94	1.13	0.49	0.00

The in-memory (page-cache) eye is the decisive one and is correlated EARLY: three coherent eyes already strip the majority of the effect (2.94 -> 1.13), matching the operational heuristic that a small number of coherent behavioural signals suffices. The precise statement is "cover the damage direction", not "three is magic".

7. Spread Implants and the Coherent Ceiling (T-MEM-3)

T-MEM-3 [T] (coordination-stealth duality on memory). An implant that spreads a fixed coherent effect E over N per-region or per-core vantages -- a low-and-slow injector touching many regions, a spread cryptominer pinning 1/N of its load per core -- keeps the COHERENT aggregate mean at sqrt(E), constant in N, while each single region or core sees only sqrt(E/N), which collapses toward the false-alarm rate.

Receipt witness (E = 36, z-threshold tau = 4):

N:	1	4	16	64	
coherent power:	0.9772	0.9772	0.9772	0.9772	(flat)
single power:	0.9772	0.1587	0.0062	0.0006	(collapse)
coherent adv:	0.00	3.00	4.50	5.25	

A fixed-seed Monte-Carlo corroborates the coherent power (0.9771). Spreading defeats every per-region threshold and never the coherent eye; a single-vantage memory scanner with a per-region budget is structurally evadable while a coherent aggregate is not.

8. Eye-Silencing and the Stealth Conservation Law (T-MEM-4)

The last move of a capable implant is to SILENCE the detectors (Section 3): patch or spoof AMSI/ETW, unhook ntdll, unregister kernel callbacks via a BYOVD driver, or DKOM the EPROCESS / task list so enumeration lies.

T-MEM-4 [T] (Stealth Conservation Law). Silencing k eyes re-opens a blind subspace of dimension exactly max(0, k - rho), where the eye redundancy rho = (number of independent eyes) - n.

Receipt witness:

```
rho = 0:  k=1 -> dim 1,  k=5 -> dim 5,  k=6 -> dim 6
rho = 4:  k=1 -> dim 0,  k=5 -> dim 1,  k=6 -> dim 2
```

DEFENSIVE READING. Provision overlapping, DIVERSE eyes so that rho is at least the implant’s realistic silencing reach k; below that, redundancy absorbs the silencing and no blind dimension re-opens. A detector that watches whether its own sensors are reporting is implementing exactly this law, and the residual gap k - rho > 0 is the "known-blind" alarm a signature AV cannot raise.

9. The Reflexive Tower: RATS as the Meta-Observer (T-MEM-5)

Detecting eye-silencing requires a META-observer of the eyes’ mutual consistency. On real hosts this is the measured-boot chain: integrity measurements extended into a TPM Platform Configuration Register, appraised remotely. This is precisely the RATS architecture [RFC9334]: an Attester produces Evidence (measurements

over code and memory), a Verifier appraises it against Reference Values ([I-D.ietf-rats-corim], [RFC9393]), and a Relying Party acts on the Attestation Result; TPM-based Remote Integrity Verification [RFC9683] and the Entity Attestation Token [RFC9711] supply the concrete evidence layer.

T-MEM-5 [T] (reflexive tower). A meta-observer of the eyes catches silencing while the level-1 gap k <= rho (blind dim 0, caught). The SAME law governs the meta layer: forging the attestation evidence (k2 > rho2 at the meta level) re-opens a genuine blind dimension one level up. Security is keeping every rung’s gap k_l - rho_l <= 0; the hardware root of trust is simply the last rung currently funded.

Receipt witness: level-1 k=2=rho -> blind dim 0 (caught); meta layer

k2=2 > rho2=1 -> blind dim 1 re-opened (genuine null, residual ~1.4e-15).

Memory-resident detection that does NOT terminate in an attested root of trust is, in the limit, defeatable: the BYOVD class (Section 3) goes UNDERNEATH a user-mode EDR in the kernel, silences the eyes, and leaves no honest rung to notice -- unless an attested meta-observer

is the next rung up.

10. The Data-Processing Ceiling (T-MEM-6)

T-MEM-6 [T] (data-processing ceiling). An action taken in an UN-SCANNED memory region is a direction v in null(H_probes). Two realities x and x + v then produce IDENTICAL telemetry y = H_probes x, so by the data-processing inequality NO function g(y) -- no AI model, however large -- can separate them. Attaching one probe on that region (changing H) restores separability.

Receipt witness: |y - y'| = 0 (identical to any classifier) while the damage gap = 5.078; after adding one memory probe on the blind region, separation = 2.500.

This bounds the role of machine learning in memory-resident detection: ML is valuable for scoring WITHIN rowspace(H), but it cannot manufacture visibility into a region no eye measures. The investment that buys detection of fileless malware is INSTRUMENTATION of the live address space (memory scanning, VM-permission and thread telemetry, PMU, attestation), not a larger model over existing telemetry.

11. Non-Blinding Invariant and Silent-Effect Ceiling (T-MEM-7, T-MEM-8)

These two results answer the question "can a faster attacker -- an AI agent, or a quantum computer -- simply out-compute the detector?" The answer is no, by type, because the quantities involved carry no

computational term.

T-MEM-7 [T] (non-blinding invariant). For any action a and any H,

```
   ||P_null(H) a||^2  +  ||P_row(H) a||^2  =  ||a||^2
   stealth(a)         +  effect(a)         =  ||a||^2
```

This is the Pythagorean identity of the orthogonal split R^n = rowspace(H) (+) null(H): every unit of stealth is a unit of effect that LEAVES the observable space. With a full-rank, redundant eye-set (rho >= 1) the null space is empty, so an in-memory implant can hide NOTHING while keeping a nonzero effect; a SILENT blinding

therefore requires either silencing k > rho eyes (which the Stealth Conservation gap reports -- "blind" implies "known-blind") or forging an eye’s authenticated identity.

Receipt witness: effect 2.940 + stealth 3.6e-15 = ||a||^2 2.940 (Pythagorean identity to 1e-9); with k <= rho the hidden effect stays 0 (caught), and only k > rho (gap 1) opens a hidden component.

T-MEM-8 [T] (silent-effect ceiling + compute invariance). The largest coherent effect deliverable while the coherent detector stays quiet is E < tau^2, for ANY spread N and ANY strategy: the region {large effect, detector silent} is EMPTY. Moreover the ceiling tau^2 and the detectability ||P_row a||^2 / sigma^2 contain no computational variable; swept over a compute budget of 30 orders of magnitude they are literally constant.

Receipt witness: E_silent_ceiling = tau^2 = 16.0 for N in {1, 4, 16, 64, 1024} (all equal); detectability constant = 10.81 across compute budget 1e0..1e30.

CONSEQUENCE. A faster search (more FLOPs, a larger model, more qubits) moves attacker and defender along the SAME information frontier without moving the boundary. AI makes the attacker OPTIMAL, not omnipotent; the optimum still loses by a margin fixed by the geometry of H. The only non-information move left -- forging a vantage -- is a cryptographic problem addressed by post-quantum eye identity (Section 16).

12. Mapping to RATS Roles and Reference Values

The receipt records the following mapping, offered so that an MVPS-Memory deployment can be described in standard RATS [RFC9334] terms:

- Attesting Environment: the in-host memory/hardware eyes (in-memory code scan, VM-permission monitor, ETW thread provider, PMU, TPM) measuring code/memory.
- Evidence: the per-tick coherence vector y = H x, conveyable as an EAT [RFC9711].
- Verifier: the MVPS coherent detector plus reflexive-integrity appraisal (joint D^2 vs single max-z; gap k - rho).
- Attestation Result: COHERENT / INCOHERENT verdict plus the localised offending entity.
- Relying Party: the response layer (alert | active), off by default.
- Reference Values: the commissioning baseline plus signed CoMID/CoSWID reference values in a CoRIM [I-D.ietf-rats-corim], [RFC9393].

MVPS-Memory defines no new RATS protocol elements; it is a profile of how to populate and appraise existing ones for memory-resident-malware detection (Section 17).

13. Numerical Receipt

All [T] claims in Sections 5-11 are exercised by

```
python scripts/validate_memory_coherence.py
```

which is pure-NumPy, deterministic (seed 20260603), uses exact Gaussian tails (one fixed-seed Monte-Carlo only to corroborate the

T-MEM-3 coherent tail), and writes evidence/memory_coherence_receipt.json. Expected output is "Total: 8 Passed: 8 Failed: 0", the T-MEM-2 eta/value sweep (0.9167/2.94 -> 0.5833/0.00), the T-MEM-3 advantage 0.00 -> 5.25 with flat coherent power 0.9772, the T-MEM-4 max(0,k-rho) grid, the T-MEM-5 caught-then-reopened meta staircase, the T-MEM-6 identical-telemetry witness (|y - y′| ~ 0), the T-MEM-7 Pythagorean identity, and the T-MEM-8 N-invariant ceiling tau^2 with compute-invariant detectability.

The receipt carries a body hash over its canonical content (excluding the timestamp):

body_sha256 =
96c6962160abd77d2afb04158a44daf83f531a00a8cc3abcf6f6a288e7922a0e

Any party can re-run the validator and compare the hash.

14. Conjectures and Falsification Protocols

C-MEM-1 [C] (lead-time before privilege completion). On a host instrumented with the in-memory and VM-permission eyes, the coherent detector raises an INCOHERENT verdict before the token/UID-0 transition completes, yielding a positive expected lead time over a per-signal detector. The test is a paired lead-time comparison vs a per-signal EDR baseline (Wilson 95% lower bound on the gain > 0) on a

labelled fileless-injection capture corpus with per-eye timestamps.

C-MEM-2 [C] (irreducible memory blind subspace). Under a realistic eye budget, determine whether an eye-set exists with rank(H) = n over the damage-relevant subspace of a curated implant corpus, or whether resource limits leave an irreducible null(H). Submodularity of rank(H) suggests a (1 - 1/e) greedy schedule of which probes to attach.

These conjectures MUST NOT be cited as guarantees.

15. Operational Considerations

An MVPS-Memory deployment SHOULD attach, at minimum, eyes covering the damage directions of the implant classes it cares about: an in-memory code/region scanner (the decisive page-cache eye), a VM-permission monitor (W^X / RX->RWX), a thread-start provider for unbacked executable memory, a credential/token hook, a KERNEL

DRIVER-LOAD eye (against BYOVD, Section 3), and per-core PMU counters for spread effects. These eyes SHOULD be appraised jointly by a coherent detector, not scored in isolation.

The reflexive-integrity layer (Section 8) MUST treat a silenced or inconsistent eye as a first-class signal, and SHOULD terminate the tower in an attested root of trust (Section 9). Per-tick verdicts and per-eye residuals SHOULD be persisted to a tamper-evident operational log [I-D.melegassi-opsawg-mvps-logging].

This document describes a host/endpoint detection profile; it does not mandate a kernel agent. A user-mode implementation cannot observe early boot and can itself be silenced by kernel-level malware (Section 3); production deployments SHOULD use kernel-level eyes and self-protection for the high-value coordinates.

16. Security Considerations

MVPS-Memory is a defensive detection-and-localisation profile. It raises alarms and identifies likely-offending entities; it does NOT actuate, quarantine, or remediate.

The central security property is geometric: an implant confined to null(H) of the attached eyes is undetectable by ANY appraisal of those eyes' output (T-MEM-6, T-MEM-8). Coverage of the damage directions of the threat model is therefore a security requirement, not a tuning choice; commissioning SHOULD verify that the eye-set spans the curated damage-direction corpus.

An implant that silences k eyes re-opens max(0, k - rho) blind dimensions (T-MEM-4); deployments MUST provision eye redundancy rho at least equal to the silencing reach they defend against, and MUST

anchor the meta-observer in an attested root of trust [RFC9334] [RFC9683] so that eye-silencing is itself observable (T-MEM-5).

POST-QUANTUM EYE IDENTITY. By the non-blinding invariant (T-MEM-7) the only attacker move that is NOT bounded by the information geometry is forging a vantage's authenticated reports so that H is mis-estimated. Each eye's Evidence MUST therefore be cryptographically bound to a hardware-rooted key. For long-lived deployments that key SHOULD use a post-quantum signature -- ML-DSA

[FIPS204] -- carried via COSE/JOSE [I-D.ietf-cose-dilithium] for EAT/CoRIM evidence and via X.509 [RFC5280] [I-D.ietf-lamps-dilithium-certificates] for the eye-identity certificate chain. The 2025-2026 BYOVD threat (Section 3) empirically confirms the split: real attackers REUSE valid signatures on vulnerable drivers rather than forge them, so the forgery channel is already economically closed and the residual attack is the geometric eye-silencing one this profile is built to flag.

A spoofed eye is an adversary-controlled row of H and can both hide damage and forge it; telemetry ingestion MUST be authenticated. The Byzantine-robust aggregate (geometric median, breakdown point 1/2) used by the Verifier bounds the influence of a minority of lying eyes, but a majority of corrupted eyes is out of scope.

This profile does not by itself remediate the underlying vulnerability an implant exploits; coherent detection is a compensating control alongside patching, exploit mitigations (W^X, CET/CFG), driver allow-listing, and attested boot.

17. IANA Considerations

This document has no IANA actions.

18. References

18.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC9334] Birkholz, H., Thaler, D., Richardson, M., Smith, N., and W. Pan, "Remote ATtestation procedureS (RATS) Architecture", RFC 9334, DOI 10.17487/RFC9334,

January 2023, <https://www.rfc-editor.org/info/rfc9334>.

18.2. Informative References

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation

List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[RFC9393] Birkholz, H., Fitzgerald-McKay, J., Schmidt, C., and D. Waltermire, "Concise Software Identification Tags", RFC 9393, DOI 10.17487/RFC9393, March 2023, <https://www.rfc-editor.org/info/rfc9393>.

[RFC9683] Fedorkow, G., Voit, E., and J. Fitzgerald-McKay,

"Remote Integrity Verification of Network Devices Containing Trusted Platform Modules", RFC 9683, DOI 10.17487/RFC9683, October 2024, <https://www.rfc-editor.org/info/rfc9683>.

[RFC9711] Lundblade, L., Mandyam, G., O'Donoghue, J., and C. Wallace, "The Entity Attestation Token (EAT)", RFC 9711, DOI 10.17487/RFC9711, 2025, <https://www.rfc-editor.org/info/rfc9711>.

[FIPS204] National Institute of Standards and Technology, "Module-Lattice-Based Digital Signature Standard", FIPS PUB 204, DOI 10.6028/NIST.FIPS.204, August 2024.

[I-D.ietf-rats-corim]
Birkholz, H., Fossati, T., Deshpande, Y., Smith, N.,

and W. Pan, "Concise Reference Integrity Manifest", Work in Progress, draft-ietf-rats-corim.

[I-D.ietf-cose-dilithium]
Prorock, M., Steele, O., Misoczki, R., Osborne, M., and C. Cloostermans, "ML-DSA for JOSE and COSE", Work in Progress, draft-ietf-cose-dilithium.

[I-D.ietf-lamps-dilithium-certificates]
Massimo, J., Kampanakis, P., Turner, S., and B. Westerbaan, "Internet X.509 PKI - Algorithm Identifiers for ML-DSA", Work in Progress, draft-ietf-lamps-dilithium-certificates.

[I-D.melegassi-opsawg-mvps-os-host]
Melegassi, L., "MVPS-Host: Canonical Multi-Vantage

Coherence Monitoring of Operating-System Fleets via Telemetry", Work in Progress, draft-melegassi-opsawg-mvps-os-host-00.

[I-D.melegassi-irtf-mvps-methodology]
Melegassi, L., "An Adversarial-Audit Methodology for

MVPS Claims", Work in Progress.

[I-D.melegassi-opsawg-mvps-logging]
Melegassi, L., "An Append-Only, Hash-Chained Operational Log Format for MVPS", Work in Progress.

Informative, non-IETF: MITRE ATT&CK techniques T1055 (Process Injection), T1562.001 (Impair Defenses: Disable or Modify Tools), T1014 (Rootkit), T1068 (Exploitation for Privilege Escalation); CVE-2025-68947 (BYOVD kernel-mode process termination).

Author’s Address

Leonardo Melegassi
Catellix
Brazil
Email: melegassi@catellix.com