How Unassigned Addressing Created a New Attack Vector: An Analysis of Dormant Autonomous System Exploitation in Backbone Internet Infrastructure

Backwater Forensics | Lu Anne Gammage (Esposito), MS Digital Forensic Science | Draft — 2026-08-25

Status: Working draft. All eight sections in progress/complete.

1. Executive Summary

Autonomous System (AS) numbers that go dormant after a carrier acquisition, bankruptcy, or internal retirement are conventionally treated as administrative debris — bookkeeping left uncorrected, not a security concern. This paper argues that treatment is wrong for a specific, testable reason: dormant ASN space with no accountable current operator is address space with no one positioned to notice or contest unauthorized use of it, and that gap is not merely untidy, it is exploitable. This is not a novel theoretical claim; the technique is independently documented in prior academic research (Testart et al., 2019; Nemmi et al., 2021) and by network-security researchers tracking real-world cases (Guilmette, 2018; Madory, 2018). This paper's contribution is a sustained, case-study-depth investigation of the pattern operating against real backbone infrastructure, built on a six-year arc from on-the-ground observations to a confirmed, evidence-graded finding set.

Methodology. The investigation applies a null-hypothesis-first standard throughout: any candidate ASN is presumed to reflect ordinary post-acquisition administrative lag until the evidence clears a specific bar (Section 2.4, Section 3). That bar is a five-tier confidence framework (Inferred, Digital Recon Affirmed, Remote Forensic Confirmed, Ground Conditions Confirmed, Active Exploit Confirmed) and a three-part digital validation pipeline — passive DNS fingerprinting, RDAP authorization checks, and BGP routing/upstream analysis — with

confirmation requiring at least one validation level to independently clear its own evidentiary standard.

Findings. Applied to a 24-ASN evidence base, this standard cleared roughly as many candidates as administrative lag as it confirmed as anomalous — a null hypothesis doing real analytical work rather than functioning as a formality (Section 4.2). The confirmed cases include a specific, repeatable cross-ASN signature predicted by the thesis: the same non-carrier secondary-market sub-allocator (Cloud Innovation Ltd / LARUS-SERVICE-MNT) appearing in the dormant space of two unrelated carrier ASNs — AS11427 (Charter/TWC lineage) and AS7029 (Windstream lineage) — with no acquisition-history explanation connecting them (Section 4.1). A separate ASN, AS7046, was investigated as a candidate third-party-control finding and did not clear that bar on further evidence — its upstream relationships confirm normal, active Verizon operation, consistent with its RFC 2270 customer-aggregation registration. A malicious domain was independently found resolving into its address space regardless, which this paper reports as an impact finding (Section 5.3) rather than a stewardship-gap finding.

Impact. For end users, the consequence of this structural gap is not abstract: inherited IP reputation from unrelated prior tenants, and routing paths through international infrastructure inconsistent with a domestic subscriber's reasonable expectations. Separately, and independent of the stewardship-gap thesis, a malicious domain was found resolving into actively-operated carrier customer space (Section 5.3) — evidence that this kind of exposure is not limited to dormant or unstewarded ASNs. In the documented stewardship-gap cases, the structural cause is consistent: no party is accountable for the space, so no clear remediation path exists when something goes wrong.

Contribution and open question. This paper's findings independently corroborate a pattern separately identified in academic literature (Testart et al., 2019; Nemmi et al., 2021; NIST, 2019) located only after this investigation's methodology and empirical work were substantially complete (Section 2.2) — convergent validity from two unrelated efforts, not a study designed around prior work. A question this paper's own review process surfaced, and does not yet have data to answer: when a routing anomaly is investigated at a distance, how often does what looks like a real event turn out to be a monitoring-instrument artifact rather than a genuine change in the network? Section 4.4 documents one case where this distinction mattered directly.

2. Thesis and Principles of the Research

2.1 Origin of the Inquiry

This investigation began as a set of on-the-ground and online observations directed at specific victims. Those early observations are not themselves evidence for the argument this paper makes — per this project's evidentiary standard, physical and single-source observations are discovery triggers, not findings — but they are the reason a backbone-infrastructure investigation was opened at all. The zoom-in they prompted led to a broader question: was the routing behavior observed around those cases idiosyncratic to those targets, or was it an instance of a general, repeatable condition in how the internet's backbone handles address space that carriers have stopped actively managing?

Over six years, that question narrowed from "something is wrong with this specific routing" to a testable, general claim about a structural property of Autonomous System (AS) allocation and BGP routing: that unassigned, dormant, or administratively orphaned address space is not merely untidy bookkeeping, but a distinct and exploitable attack surface.

2.2 Thesis

Dormant and unassigned Autonomous System space constitutes a persistent, exploitable attack vector in backbone internet infrastructure — separate from and not fully explained by ordinary post-acquisition administrative lag — because the absence of active stewardship removes the one control (an attentive registrant) that would otherwise detect and contest unauthorized routing.

This is not a novel theoretical claim in isolation. It is independently documented in the academic literature: Nemmi et al. (2021) identify dormant ASNs "suddenly waking up" to hijack address space, citing AS10512 — allocated for 17 years, active in BGP for only 31 days, during which it hijacked 60 /16 prefixes including space belonging to Spectrum (AS11426). Testart et al. (2019) trained a classifier that flagged 934 ASes with behavioral similarity to known serial hijackers. NIST SP 800-189 formally names both "announcement of unallocated address space" and "prefix squatting" as interdomain routing attack patterns. This paper's contribution is not to establish that the technique exists — the literature already does that — but to document its operation, at case-study depth, against real backbone infrastructure over a sustained investigation, and to

show a specific repeatable signature: the same non-carrier secondary-market sub-allocator appearing across multiple, otherwise-unrelated dormant carrier ASNs.

A note on chronology, stated plainly for methodological honesty. This investigation's methodology, hypothesis, and the confirmed findings reported in Section 4 were developed and largely completed before this academic literature was located. The literature above was found during the drafting of this paper — after the empirical work, not before it — and its role here is independent corroboration that this project's findings match a pattern separately documented by academic researchers using different methods and a different dataset, not a framework this investigation was designed against. That distinction matters: a finding that happens to match prior literature discovered afterward is evidence of convergent validity, not evidence that the investigation was built to reproduce a known result. The remainder of this paper is written to keep that distinction clear — the literature is cited as corroboration, never as a source the methodology was derived from.

2.3 What This Paper Is Not Arguing

Per the Designation Gate applied throughout this project's methodology, no actor or entity is named as culpable in this paper unless the evidentiary bar for that claim is independently cleared and documented. This paper describes **infrastructure conditions** — what address space is being announced, by what AS, with what (or absent) registration authority — not intent, and not attribution to a named actor beyond what ARIN/RDAP records establish as a matter of public record. Where a carrier's own ASN shows an anomaly (e.g., Charter appearing under three different status classifications across its ASN portfolio), the paper's default explanation is administrative lag until the evidence clears the higher bar described in Section 2.4.

2.4 The Null Hypothesis This Paper Had to Clear

Large carriers accumulate ASNs through decades of acquisition (TCI → AT&T Broadband → Comcast; Time Warner Cable → Charter; MCI → Worldcom → Verizon Business; Global Crossing → Level 3 → Lumen). A dormant or inconsistently-documented ASN is the expected byproduct of that history, and by itself proves nothing. The working null hypothesis throughout this investigation has been:

H0 — Administrative Lag: Apparent routing anomalies in legacy carrier ASNs are fully explained by ordinary post-acquisition record-keeping delay. No unauthorized third party is routing the

space; the registrant's own network engineering has simply not caught up to ARIN's records, or vice versa.

H0 is the default explanation for any single anomalous observation in this dataset. It is only set aside for a given ASN when the evidence clears one of the Tier R (Remote Forensic Confirmed) confirmation standards described in Section 3 — not on the basis of the anomaly's appearance alone. Section 3.4 documents the specific evidentiary bar and gives a worked example (AS10913) of a finding that was tested against H0, found to be H0 after all, and retracted — which the project methodology treats as the process working correctly, not as an error to be minimized.

2.5 Guiding Principles

The research adheres to the following principles, carried consistently across all evidence collection, characterization, and disclosure activity described in Section 3–5:

Principle	Application
Actor-agnostic framing	Findings describe infrastructure conditions ("AS11427 announces prefixes it has no recorded authorization for"), not actors or motive.
Evidence-graded claims	Every finding is traceable to a named source, database query, or documented OSINT method, and carries an explicit confidence tier (Section 3.2).
Reproducibility	Methodology is public-tool-based (ARIN RDAP, RIPEstat, Robtex) and explicit enough that an independent researcher with the same access could reach the same findings.
Partner-oriented disclosure	Carriers and CISA are treated as partners in remediation, not subjects of accusation. Disclosures give carriers a remediation window rather than asserting wrongdoing.
Null-hypothesis-first	The benign/administrative explanation is stated and evaluated before any anomaly label is applied (Designation Gate).
Cleared findings are retained	A finding that does not hold up (e.g., AS10913, Section 2.4) is documented as a retraction, not deleted — clearing a lead is treated as evidentiary output in its own right.

3. Experiment Structure, Hypothesis, and Methodology

3.1 Formal Hypotheses

H1 (working hypothesis): A measurable subset of dormant or under-stewarded Autonomous System space is being used to route address blocks without documented authorization from the registrant, and this activity follows a repeatable pattern rather than occurring as isolated, unrelated incidents.

H0 (null hypothesis): Observed anomalies in legacy carrier ASN routing are attributable to ordinary administrative lag following corporate acquisition, with no unauthorized third-party routing activity present.

H1 is accepted for a given ASN only when at least one Tier R confirmation standard (Section 3.4) is independently met. Meeting a lower evidentiary tier (Inferred or Digital Recon Affirmed) is not sufficient to reject H0 for that ASN; it moves the item to the validation queue rather than to a confirmed finding.

3.2 Confidence Tier Framework

All findings in this investigation are graded against a five-tier confidence scale, applied consistently from initial discovery through final characterization:

Tier	Code	Meaning
Inferred	I	Acquisition history predicts a seam condition — not directly observed
Digital Recon Affirmed	D	Passive OSINT confirms conditions favorable to the hypothesis
Remote Forensic Confirmed	R	PCAP, live BGP behavior, passive DNS, or ARIN/RDAP verification — forensic-grade digital evidence
Active Exploit Confirmed	A	Direct, first-hand confirmation of active exploitation — victim report, ISP action, or law enforcement action (including seizure/sinkholing of address space) — analyst-assigned only, never automated

This paper applies four of the five Backwater Forensics confidence tiers (I, D, R, A). Ground Conditions Confirmed (G) is part of the parent framework but was not a confirmation pathway used in this investigation; backbone/ASN findings moved directly from Tier R (digital) to Tier A (direct law enforcement action, including seizure/sinkholing) with no intervening physical/case-overlap corroboration step.

This paper reports findings at Tier R or above only, consistent with the confirmation standard described below. Lower-tier items (I, D) are described in Section 4 as candidates under monitoring, not as confirmed findings.

3.3 Validation Pipeline

The investigation proceeds through a phased pipeline, moving a candidate ASN from initial discovery to a confirmed disposition:

Phase A — Initial validation via RIPE/ARIN RDAP lookup (registrant identity, allocation date, basic routing presence)
Phase B — Digital risk assessment (prefix count, pDNS presence, upstream transit relationships)
Phase C — PTR / routing validation (confirmation-grade checks described in 3.4 below)

A candidate ASN is not reported as confirmed until it has passed through Phase C and cleared at least one Tier R standard.

3.4 Tier R Confirmation Standards (Validation Levels 3–5)

Note on terminology: "Validation Level" (below) refers to which diagnostic test was run in the validation pipeline. It is a separate axis from the confidence tiers (I, D, R, A) defined in Section 3.2 — a finding can pass Validation Level 4 (RDAP) and still only carry Tier R confidence until further corroborated. The two are related but not interchangeable.

Three independent diagnostic tests are available to move an ASN from `PENDING_VERIFICATION` to a confirmed status. Any single test meeting its confirmation standard is sufficient to confirm at Tier R; all three meeting standard together constitutes the strongest evidentiary basis.

Level 3 — Passive DNS Fingerprint. Tests whether the ASN's announced IP space resolves to live carrier infrastructure hostnames, dormant space, or anomalous/foreign hostnames inconsistent with the ASN's documented carrier history. Confirmed when carrier-infrastructure hostnames resolve from space the ASN has no documented right to announce, or when foreign/anomalous hostnames resolve from ostensibly domestic carrier space. Tooling: `asn_pdns_puller.py` against RIPEstat (prefix enumeration) and Robtex (passive DNS), no authentication required.

Level 4 — RDAP OriginAS Authorization Check. Tests whether any ASN is authorized by the IP block's registrant to announce that space. An empty `originas` field on the ARIN RDAP record means no ASN — including the one currently routing the block — has documented authorization. Confirmed when sampled blocks return `originas: []`, or when the registrant of record is a non-carrier entity with no documented acquisition chain to the announcing ASN. Data source: ARIN RDAP (public, read-only).

Level 5 — BGP Prefix and Routing Analysis. Tests whether current announced prefix composition and upstream transit relationships are consistent with the ASN's documented history. Confirmed when international backbone upstreams appear for a domestic-only carrier ASN with no documented international operations, when prefix composition includes geographically inconsistent space, or when two independently dormant ASNs share an identical upstream set (indicating common operational control rather than coincidence). Data source: RIPEstat (public, read-only). A secondary, non-dispositive check cross-references the RIPE Internet Routing Registry (IRR) for a registered routing policy; absence of one is a supporting flag, not independent confirmation.

3.5 Sampling Frame

The candidate population was seeded from a set of geographic nodes (ZIP-code-based) associated with the six-year investigation's original discovery triggers, subsequently expanded to include university-network nodes as a comparison subset. ZIP-code seeding is used strictly as a sampling method to identify which carrier ASNs serve a given locality for further RDAP/BGP analysis — it is not itself evidentiary, and no physical-location finding is reported in this paper's scope (Autonomous System routing conditions only, per project scope decision).

The sampling frame grew across three points in the investigation rather than being fixed from the outset. The 2026-05-05 baseline register comprised 19 ASNs, spanning legacy TCI/AT&T Broadband, Adelphia/Insight, Time Warner Cable/Charter, MCI/Worldcom, Global Crossing/Level 3, EarthLink/Internap, and Windstream lineages — chosen because each represents a distinct acquisition chain with a plausible dormancy or stewardship gap. That register was subsequently expanded to 23 ASNs through registry expansion (Section 8.3), and to the paper's full 24-ASN evidence base with the later addition of AS7046, which entered the investigation through a separate thread — the bybanking.com sinkhole discovery (Section 4.3) — rather than the

original acquisition-lineage sampling logic above. The count reported elsewhere in this paper (Executive Summary, Sections 4.0, 4.2, and 8) is this final, fully reconciled 24.

3.6 Corroboration Threshold

A three-independent-hit threshold applies to cyber/network evidence: three independent cyber/network findings (e.g., pDNS anomaly + RDAP gap + shared upstream with another anomalous ASN) confirm a pattern as deliberate rather than coincidental, where a single hit alone would not. This threshold applies only to cyber/network evidence; it does not apply to and is not satisfied by physical/on-the-ground observations, which are excluded from this paper's evidentiary base by design (Section 3.5).

3.7 Data Sources

Source	Role	Access
ARIN RDAP	Registrant identity, allocation history, originas authorization	Public, read-only
RIPEstat	Announced prefixes, routing status, ASN upstream neighbors	Public, read-only
Robtex	Passive DNS	Public, read-only
RIPE IRR	Routing policy registration (secondary flag)	Public, read-only
CISA supplemental filings	Disclosure and correction record for filed findings	Internal case record

3.8 Methodological Limitation Acknowledged in the Literature

Academic literature located after this investigation's methodology was developed (see the chronology note in Section 2.2) independently corroborates a limitation this project encountered directly: BGP-activity analysis alone cannot fully distinguish malicious squatting from other causes without administrative allocation context. Nemmi et al. (2021) note that some dormant-ASN awakenings (e.g., 31 ASNs reactivating simultaneously in April–July 2020) were

only confirmable as malicious by cross-referencing known-malicious upstream ASNs, not from prefix behavior in isolation. This investigation's combination of the RDAP originas check and BGP upstream analysis (Section 3.4, Validation Levels 4 and 5) was designed independently and happens to address the same limitation.

4. Findings

4.0 Overview

Findings are organized thematically rather than ASN-by-ASN, consistent with the thesis in Section 2: the paper's contribution is the *pattern*, not any single ASN's status. Full per-ASN evidence, dates, and file references are in Section 8. This section draws on that evidence base to make three arguments in sequence: that the cross-ASN signature predicted in Section 2.2 is present in the data; that the null-hypothesis discipline in Section 2.4 actually separated administrative lag from exploitation rather than assuming the answer; and that a candidate third-party-control finding (AS7046) was investigated and, on further evidence, did not hold up — retained here as an example of the discipline working, not deleted, per Section 2.5.

4.1 The Cross-ASN Signature Holds

Section 2.2 proposed a specific, falsifiable signature distinguishing systematic exploitation from ordinary administrative lag: the same non-carrier secondary-market sub-allocator appearing across multiple, otherwise-unrelated dormant carrier ASNs. That signature is confirmed in one instance and supported by a second, pending independent verification.

AS11427 (TWC-11427-TEXAS, Charter's own ARIN registration, BGP routing authority unknown) carries a prefix composition of 21% legacy Time Warner Cable space, 77% Cloud Innovation Ltd (Seychelles, AFRINIC secondary-market registrant ORG-CIL1-AFRINIC), and 2% APNIC space under MAINT-SNPL-PK (Pakistan). A subset of that space — the 156.x.x.x range — is AFRINIC ERX: unallocated registry-held blocks being announced with no end-user allocation on record.

AS7029 (Windstream, WINDSTREAM_RECLAIM status following its own reclaim confirmation) is separately associated with a 154.194.16.0/21 block registered to Future Tech Distribution under the same sub-allocator, LARUS-SERVICE-MNT — an association documented in this project's correction log but not yet independently confirmed by a block-level RDAP query (Section 8.1b);

treated here as a supporting data point pending that confirmation, not as an independently verified second instance of the signature.

One carrier ASN — AS11427 — carries a confirmed, RDAP-verified instance of address space from a Seychelles LIR (Cloud Innovation Ltd / LARUS-SERVICE-MNT) routed through its dormant allocation, with no acquisition-history explanation connecting that LIR to Charter/TWC. AS7029's association with the same sub-allocator is documented in this project's own correction log but rests on a source that has not yet been independently confirmed by a block-level RDAP query (see the note above and Section 8.1b); it is reported here as a lead consistent with the same pattern, not as a second confirmed instance. If independently confirmed, the two together would represent unrelated carrier ASNs — unrelated acquisition histories (Charter/TWC vs. Windstream), unrelated geographies, unrelated original owners — carrying address space from the same external sub-allocator, which post-acquisition record-keeping delay alone would not explain. Until that confirmation exists, this paper's falsifiable claim rests on the single verified AS11427 instance; the AS7029 lead is disclosed for transparency and flagged for the next validation pass, not treated as established. This finding is consistent with, and — pending AS7029's confirmation — would add a case instance to, the "systematic routing vehicle" pattern documented by Nemmi et al. (2021) in dormant-ASN hijacking generally.

4.2 The Null Hypothesis Did Real Work

A methodology that never clears H0 for anything is not rigorous — it is unfalsifiable. Table 4.1 shows the null hypothesis was applied evenhandedly across the 24-ASN evidence base (Section 8), clearing roughly as many candidates as it held.

Table 4.1 *Disposition of Candidate ASNs Against the Administrative-Lag Null Hypothesis*

Disposition	ASNs	Basis
H0 held — cleared as administrative lag / misattribution	AS10913, AS6181, AS2686, AS5650	Direct RDAP registrant confirmation contradicted the working hypothesis in each case (Section 8: AS10913 retraction, CISA CORRECTION-002; AS6181 Cincinnati Bell/FUSE-NET, corrected pre-disclosure; AS2686/AS5650 confirmed legitimate current operators via RDAP + RIPEstat)
H0 held — investigated as candidate third-party control, confirmed normally operated	AS7046	Registered `RFC2270-UUNET-CUSTOMER`; upstream peer data confirms active Verizon operation (three of five upstream peers are Verizon Business/MCICS-registered sibling ASNs; see 4.4 and 8.1b). A malicious domain was independently found in its address space regardless — reported as an impact finding (Section 5.3), not as evidence this ASN is unstewarded
H0 rejected — Tier R confirmed third-party exploitation	AS11427, AS7015	Cleared the Tier R confirmation standard (Section 3.4): originas gaps or routing/upstream anomalies indicating unauthorized third-party control inconsistent with documented history
H0 rejected — Tier R confirmed, administrative retention anomaly (no third-party control)	AS11426, AS6128	Carrier retains a redundant or duplicate legacy ASN with no operational handoff to a third party; anomalous relative to documented acquisition history but not evidence of unauthorized routing

Disposition	ASNs	Basis
H0 rejected — status conflict, not independently resolved	AS8069	Active anomaly since the 2026-05-05 baseline (`OWNERSHIP_ANOMALY`, listed among ASNs requiring disclosure/action) — never cleared. Two later sources disagree on its current label (`ZOMBIE-ASN-REGISTRY.db`: `ACTIVE_MONITOR`; `asn_source.json`: `MISATTRIBUTION`, frozen 2026-05-06); PeeringDB confirms the registrant (Microsoft Azure Routing Preference) regardless of which label is current. Carried forward as unresolved, not picked one way or the other — see 8.1c
Resolved during drafting — corrected, not left pending	AS33363 (→ RETENTION_ANOMALY), AS54396 (→ MISATTRIBUTION)	Register cross-check (`ZOMBIE-ASN-REGISTRY.db`) caught two stale statuses in this paper's own earlier draft — see Section 8 entries

Two of the paper's clearances — AS10913 and AS6181 — are worth naming specifically because they show the discipline catching itself at different points in the disclosure pipeline. AS10913 was filed to CISA as a confirmed zombie on 2026-05-02 and retracted three days later (CORRECTION-002) — the correction happened, but only after external disclosure. AS6181 was headed for the same filing, built on a full write-up (geography, upstream peers, a 14-year "double migration failure" narrative) — and was caught and corrected internally before it ever reached CISA or FBI. Methodologically these are the same discipline; operationally, the second is the better outcome, since it demonstrates the check working *before* an error reaches an external partner rather than after.

4.3 AS7046 — Investigated as a Candidate Finding, Redirected on Further Evidence

An earlier draft of this paper treated AS7046 as a third-party-control finding parallel to AS11427 and AS7015 — dormant, unstewarded federal address space, occupied by unrelated malicious

infrastructure. On round-1 peer review and a subsequent evidence recheck (2026-08-25), that framing did not hold up, and per the "cleared findings are retained" principle (Section 2.5), the retraction is documented here rather than the section simply disappearing.

Two things changed the assessment. First, AS7046's registration (`RFC2270-UUNET-CUSTOMER`) describes a specific, ordinary function — a shared ASN a provider uses to originate its single-homed customers' address blocks — under which continuous, fully-visible routing is the *expected* state, not evidence of a stewardship gap. Second, and more directly: a fresh RIPEstat upstream-neighbor query (2026-08-25) found that three of AS7046's five upstream peers are themselves Verizon Business/MCICS-registered sibling ASNs, and the dominant relationship by a wide margin is AS701 — Verizon's own UUNET backbone (Section 8.1b). That is not consistent with third-party or unauthorized control; it is what a normally-operated carrier customer-aggregation ASN's upstream table looks like.

A malicious domain was independently found resolving into AS7046's address space regardless of this reclassification — that finding did not depend on AS7046 being dormant, and is retained and reported in full as an impact finding (Section 5.3), not as evidence for this paper's stewardship-gap thesis.

4.4 A Retracted Timing Correlation, and What Actually Happened

An earlier draft of this paper argued that AS7015's and AS7046's routing disruptions coincided with a real, externally documented takedown operation announced 2026-05-18, treating that coincidence as corroborating (though not dispositive) context. On round-1 peer review, that claim was rechecked directly against the analyst's own contemporaneous monitoring records rather than against the paper's later summary of them — and it did not hold up.

For AS7015: the analyst's own working notes from 2026-05-22, written the same week and before any "dark window" framing existed, state plainly that AS7015's prefix count was "stable at 121 (timeout streak cleared — **NOT going dark**; status: ZOMBIE_TRANSIT restored)." What actually occurred was a series of RIPEstat query timeouts, compounded by a documented, multi-day automated-monitoring failure (`MONITOR FAILURE — sandbox 403`) affecting the pipeline broadly — including AS7922, a CLEAN control ASN, on the same dates. When a manual query finally succeeded, AS7015's count matched its pre-window baseline exactly. This is not consistent with a real routing withdrawal; it is consistent with the monitoring instrument failing and then recovering. AS7015's Tier R finding (originas gaps, upstream inconsistency identified at the

2026-05-05 baseline) is unaffected by this correction and stands on its own evidentiary basis — see Section 8.1b. What is retracted is only the later dark-window/timing-correlation claim.

For AS7046: this investigation's monitoring of the ASN began on 2026-05-19 — meaning there is no prior baseline against which a "went dark" transition could have been observed. The claim described an assumed transition, not an observed one. Combined with Section 4.3's finding that AS7046 is a normally, continuously operated ASN, no disruption claim is made for it in this paper.

No timing-correlation claim involving this operation is made in this revision, for either ASN. This section is retained, per Section 2.5's "cleared findings are retained" principle, specifically so the correction is visible rather than the section quietly disappearing.
[Analyst note, retained for this internal review pass: whether and how the underlying operation is referenced elsewhere in this paper — as general background rather than a timing claim — is a separate, still-open editorial question, not resolved in this edit.]

5. Impact to Users

5.0 Overview

The findings in Section 4 describe an infrastructure condition. This section describes what that condition means for the people whose traffic passes through it — subscribers who have no visibility into which ASN carries their packets, no way to know whether that ASN has an accountable current operator, and no mechanism to opt out of routing through address space with the characteristics documented in Sections 4.1–4.2. Section 5.3 also reports a finding independent of that stewardship-gap thesis — evidence that this kind of exposure isn't limited to dormant or unstewarded ASNs.

5.1 Inherited Reputation

Address space does not arrive clean. AS11427's prefix composition includes AFRINIC ERX blocks and Cloud Innovation Ltd secondary-market space with routing and reputation histories entirely disconnected from the Charter subscribers whose traffic may traverse it. A subscriber has no way to know that the IP address assigned to them carries a blocklist history, spam reputation, or prior abuse association accumulated by a completely different, unrelated party before the

space was folded into a zombie-routed block. This is a direct, individual harm: legitimate traffic — email, VPN connections, authenticated sessions — can be blocked, flagged, or rate-limited by downstream services relying on IP reputation, for reasons the subscriber has no way to diagnose and no relationship with the responsible party to resolve.

5.2 Anomalous Routing Exposure

Several confirmed zombie ASNs in this investigation's evidence base show upstream transit relationships inconsistent with their documented domestic customer base — international Tier 1 peers (Telstra, PCCW, SingTel, Arelion) appearing on ASNs that, per their registration history, should carry only regional US traffic. A subscriber whose traffic is routed through such a path experiences this invisibly: added latency, additional international hops, and — more significantly — traffic traversing networks and jurisdictions the subscriber never agreed to and has no reason to expect. This is not a claim that any specific subscriber's traffic has been intercepted; it is a claim that the routing path itself is inconsistent with what a domestic residential or business subscriber should reasonably expect, and that inconsistency is invisible to the person experiencing it.

5.3 Malicious Infrastructure in Actively-Operated Carrier Space

Section 4.3 documents that AS7046 is a normally, continuously operated Verizon customer-aggregation ASN, not dormant or unstewarded. That correction does not remove the underlying observation: a domain independently flagged as malicious (`bybanking.com`) was found resolving into two of AS7046's announced address blocks, on two separate occasions two months apart, both independently confirmed via direct RIPEstat prefix-list query (Section 8.1b). This is arguably a more concerning finding than the paper's original framing, not a weaker one — it means this kind of exposure is not confined to space nobody is watching. Space that a legitimate business customer's infrastructure planning would reasonably assume is properly assigned and monitored can still surface unrelated malicious activity, with no connection to the ASN's actual operator. Any monitoring, security tooling, or threat-intelligence system that associates network behavior with the announcing ASN or its registered organization risks misattributing this activity to Verizon Business/UUNET, an organization with no operational connection to it.

5.4 Loss of Accountability

Across every confirmed finding in Section 4, the common thread is not malicious intent on the

part of the original carrier — it is the absence of anyone accountable for the space at all. A subscriber experiencing a routing or security problem traceable to zombie-routed address space has no clear party to contact: not the original carrier (which no longer operates the space and, in several cases documented in Section 8, may not know it is still routing), not the acquiring carrier (which has no visibility into space it never took over), and not ARIN (which maintains the registration record but has no operational role in troubleshooting). This is the structural harm underlying every specific example above: address space with no accountable operator produces no clear remediation path when something goes wrong, regardless of whether "something going wrong" is a reputation problem, a routing anomaly, or hosted malicious infrastructure.

6. Conclusion

6.1 What This Paper Established

The thesis stated in Section 2.2 — that dormant and unassigned Autonomous System space constitutes a persistent, exploitable attack vector separate from ordinary administrative lag — is supported by the evidence in Section 4, with the specific evidentiary bar set in Section 2.4 (the administrative-lag null hypothesis) applied consistently rather than assumed away. The cross-ASN signature predicted in Section 2.2 — the same non-carrier secondary-market sub-allocator appearing across multiple, otherwise-unrelated dormant carrier ASNs — is present in the confirmed data (Section 4.1). The null hypothesis did real analytical work rather than functioning as a formality: roughly as many candidate ASNs were cleared as administrative lag as were confirmed as anomalous (Section 4.2, Table 4.1), and three of those clearances — AS10913, AS6181, and AS7046 — demonstrate the methodology catching its own errors at different points in the process: two before and after external filing (Section 4.2), and one during peer review, after this paper was already posted publicly (Section 4.3). AS7046's retraction is, if anything, the sharper demonstration of the discipline this paper argues for: a candidate finding investigated, checked against fresh primary evidence, and corrected in public rather than left standing.

6.2 Limitations

This paper's evidence base is drawn from a single investigation's sampling frame (Section 3.5), seeded from specific geographic nodes and subsequently expanded, not from a systematic

census of all ARIN-region ASNs. The confirmed findings should be read as case-study depth on a real, bounded set of carrier ASNs, not as a population-level estimate of how common this pattern is across the internet's full address space. The methodology itself has a documented limitation (Section 3.8): BGP activity and RDAP authorization gaps alone cannot always distinguish malicious squatting from other administrative causes without the kind of cross-referencing this investigation performed — a limitation independently corroborated by academic literature located after this investigation's methodology was already in place (Nemmi et al., 2021; see the chronology note in Section 2.2). Finally, as demonstrated directly by Section 4.4's retraction, a routing anomaly observed through remote digital methods alone can be a genuine network event or a monitoring-instrument artifact, and distinguishing the two requires checking the instrument's own contemporaneous behavior — including on unrelated control ASNs — not just the anomalous ASN in isolation. This paper is explicit that it did not do so on the first pass, and that the correction only happened because the original working notes were preserved and re-checked.

6.3 A Further Question This Paper Raises But Does Not Answer

An earlier draft of this section asked whether disclosure of a vulnerable ASN produces durable remediation or only a temporary lull before reoccupation, built on AS7046 having been "disrupted once… reoccupied twice." Section 4.4's retraction removes the disruption this question depended on — AS7046 was never confirmed dark, so there is no gap to have been "reoccupied." That specific framing does not survive this revision.

A narrower, still-open question survives it: `bybanking.com` was found resolving into two different AS7046-announced blocks, two months apart, within an ASN that was continuously and normally operated throughout. Why a malicious domain would resurface twice in the same carrier's customer-aggregation space — a compromised or complicit customer, unauthorized subletting of an assigned block, or something else — is not established by the evidence in hand, and this paper does not speculate further than that. A separate limitation compounds the uncertainty: the passive-DNS tool used returned only a last-seen timestamp for both records, with no first-seen date captured (Section 8.1b) — meaning even the two-months-apart framing describes when the records were *queried*, not necessarily how long each resolution had actually been live. This paper flags both the narrower question and this evidentiary limitation; it does not have the data to resolve either.

Unassigned and dormant Autonomous System space is not a bookkeeping curiosity left over from decades of carrier consolidation. It is address space with no accountable current operator, and the evidence in this paper shows that gap gets used — by secondary-market IP brokers routing space with no legitimate end-user allocation, by unrelated criminal infrastructure taking advantage of a carrier customer ASN nobody is watching, and, at least once, by whatever disrupted that infrastructure in turn. The internet's routing system has no built-in mechanism that requires an ASN to prove it is still accountable to anyone. Until it does, this attack surface will keep being available to whoever finds it next.

7. Bibliography

Guilmette, R. F. (2018, June 26). *AS3266: BitCanal hijack factory, courtesy of Cogent, GTT, and Level3* [Mailing list message]. NANOG. https://mailman.nanog.org/pipermail/nanog/2018-June/096034.html

Kumari, W., Bush, R., Schiller, H., & Patel, K. (2015). *Codification of AS 0 processing* (RFC 7607). Internet Engineering Task Force. https://doi.org/10.17487/RFC7607

Madory, D. (2018, July 11). *Shutting down the BGP hijack factory*. Dyn Blog. https://dyn.com/blog/shutting-down-the-bgp-hijack-factory/

National Institute of Standards and Technology. (2019). *Resilient interdomain traffic exchange: BGP security and DDoS mitigation* (NIST Special Publication 800-189). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-189

Testart, C., Richter, P., King, A., Dainotti, A., & Clark, D. (2019). Profiling BGP serial hijackers: Capturing persistent misbehavior in the global routing table. In *Proceedings of the Internet Measurement Conference (IMC '19)* (pp. 420–434). Association for Computing Machinery. https://doi.org/10.1145/3355369.3355581

Nemmi, E. N., Sassi, F., La Morgia, M., Testart, C., Mei, A., & Dainotti, A. (2021). The parallel lives of Autonomous Systems: ASN allocations vs. BGP. In *Proceedings of the ACM Internet Measurement*

Conference (IMC '21), 19 pages. Association for Computing Machinery. https://doi.org/10.1145/3487552.3487838

Note: verified 2026-07-30 against the original ACM PDF (analyst-provided). Two corrections applied: (1) the author list was previously copied from the 2019 Testart et al. entry — actual 2021 authors are Nemmi, Sassi, La Morgia, Testart, Mei, and Dainotti (Testart is 4th author, not 1st). Per analyst direction (2026-07-30), all six in-text citations of this source (Sections 2.1, 2.2, 2.3, 3.8, 4.1, 6.3) have been updated from "Testart et al. (2021)" to "Nemmi et al. (2021)" to match; the 2019 paper (genuinely first-authored by Testart) is unaffected and still cited as "Testart et al. (2019)" throughout. (2) DOI confirmed correct (10.1145/3487552.3487838); ACM lists this as a 19-page article, not a continuous page range — "page range" as originally requested does not apply to this citation format. The NIST SP 800-189 citation remains unverified and is out of scope for this pass.

8. Evidence Log

Backwater Forensics | VRF#26-04-TPWXX | Culled for peer review 2026-07-29: full per-file evidence tables retained only for the six ASNs that move or control the paper's arguments (Sections 4.1–4.4); all other ASNs summarized to one row each. ***210 unique evidence files*** *remain represented in aggregate across this log (per-ASN sections plus the batch/multi-ASN summary in 8.2), deduplicated for files cross-referenced under more than one ASN. Full per-file hashes for every file — summarized or not — remain in* `SHADOW_MARKET_FILE_HASHES.txt`*, which is unaffected by this cull. 6 files excluded as out-of-scope (analyst-scoped, dated 2026-07-11) and 4 files (AS702/AS2686/AS5650/AS14905 pDNS run) confirmed in-scope as comparison/control evidence.*

8.1 Corrections on File

ASN	Correction	Filed as	Status
AS10913	TRUE ZOMBIE (filed 2026-05-02) -> LEGITIMATE_SUCCESSOR	CISA CORRECTION-002	Retracted post-disclosure
AS11427	CLEAN (Phase A) -> THIRD_PARTY_CONTROL /	CISA CORRECTION-	Corrected post-disclosure

ASN	Correction	Filed as	Status
	ZOMBIE	001	
AS6181	TRUE ZOMBIE (Insight) -> FALSE_POSITIVE (Cincinnati Bell/FUSE-NET)	Not filed — caught pre-disclosure	Corrected in baseline register 2026-05-05, before any CISA/FBI transmission. Internal record `FALSE-POSITIVE-ALERT-AS6181-CISA-SUPPLEMENT-VRF26-04-TPWXX.txt` documents the correction on Backwater Forensics' own side; its CISA-styled filename reflects the intended-format convention, not an actual transmission. No retraction required.

8.1a Analyst-Assessed Law Enforcement Activity — Retracted (see 4.4)

ASN	Finding held	Assessed event	Status
AS7015	~~ZOMBIE_TRANSIT (Tier R, 2026-05-05) → SINKHOLE_TRANSIT (Tier R)~~ → **ZOMBIE_TRANSIT (Tier R) — restored**	Previously assessed as a dark window and re-emergence timing coincident with INTERPOL Operation Ramz (~2026-05-19/22, per `BACKBONE-INVESTIGATION-LOG-v2.md` I-032)	**Retracted 2026-08-25, on peer review + direct recheck of contemporaneous notes.** The analyst's own 2026-05-22 working note states plainly: "NOT going dark; status: ZOMBIE_TRANSIT restored." What occurred was RIPEstat query timeouts compounded by a documented multi-day automated-monitoring failure (`MONITOR FAILURE — sandbox 403`) affecting the pipeline broadly, including a CLEAN control ASN (AS7922) on the same dates. No law-enforcement-timing assessment is made for this ASN in this paper. See Section 4.4 for the full retraction. The underlying Tier R finding from the 2026-05-

ASN	Finding held	Assessed event	Status
			05 baseline (originas gaps, upstream inconsistency) is unaffected and stands independently.

8.1b Full Evidence — Load-Bearing ASNs

The six ASNs below carry direct citations in Sections 4.1–4.4 and retain full per-file evidence tables.

AS6181 — FUSE-NET — Cincinnati Bell Telephone Company LLC

Status: FALSE_POSITIVE | **Case ref:** CASE-008 | **Confidence tier:** R | **Evidence files:** 3

CORRECTED PRE-DISCLOSURE. RDAP (AS6181-DEETS.txt, 2026-07) confirms registrant is Cincinnati Bell (FUSE-NET), not Insight. Attribution error caught and corrected in baseline register by 2026-05-05, before any CISA/FBI transmission. Note on provenance: the ZOMBIE-ASN-REGISTRY.db `source_ref` for this entry (`FALSE-POSITIVE-ALERT-AS6181-CISA-SUPPLEMENT-VRF26-04-TPWXX.txt`) is an internal Backwater Forensics record documenting the correction — despite the filename, it was never transmitted to CISA. Timing meant AS6181 was already resolved before any CISA filing cycle that would have included it; neither the original zombie characterization nor the correction record ever left this investigation. See correction note below.

Date	File	Type
2026-05-03	`prefixes_AS6181_20260503_170109.json`	Level 5 — BGP/Prefix
2026-05-03	`sample_ips_AS6181_20260503_170109.txt`	Level 5 — BGP/Prefix
2026-05-08	`pdns_AS6181_20260508_193449.json`	Level 3 — Passive DNS
2026-06-18	`rdap-batch-20260618_024735.txt` [shared: multi-ASN]	Level 5 — BGP/Prefix (RIPEstat routing-status; confirms AS6181 live/active, 116 prefixes)
2026-07-12	`AS6181-DEETS.txt`	**Level 4 — RDAP/WHOIS (registrant confirmation).** Direct `rdap.arin.net/registry/autnum/6181` pull. Registrant: Cincinnati Bell Telephone Company LLC (CBTL-6). Resolves the AS6181 attribution conflict definitively.

AS7015 — COMCAST-7015 — Comcast-operated TCI legacy, 159 downstream customers

Status: ZOMBIE_TRANSIT (Tier R, 2026-05-05) — **restored; dark-window/law-enforcement reclassification retracted 2026-08-25** | **Case ref:** CASE-002/003 | **Confidence tier:** R | **Evidence files:** 13

Corrected twice now. Previously written as "Tier A, FBI seizure/sinkholing" — overstated, corrected to Tier R (Section 3.2/3.4). Then, on 2026-08-25 peer review, the subsequent SINKHOLE_TRANSIT/dark-window reclassification was itself retracted: the analyst's own 2026-05-22 contemporaneous note states "NOT going dark; status: ZOMBIE_TRANSIT restored," identifying the underlying cause as RIPEstat query timeouts and a documented automated-monitoring failure (`MONITOR FAILURE — sandbox 403`) that also affected CLEAN control ASN AS7922 on the same dates — not a real routing withdrawal. AS7015's status reverts to its 2026-

05-05 baseline: ZOMBIE_TRANSIT at Tier R (originas gaps, upstream inconsistency), unaffected by this correction. See Section 4.4 and 8.1a for the full retraction record.

Date	File	Type
2026-05-05	`bgp_announced_AS7015_20260505_034213.txt`	Level 5 — BGP/Prefix
2026-05-05	`bgp_neighbors_AS7015_20260505_034115.txt`	Level 5 — BGP/Prefix
2026-05-05	`bgp_neighbors_AS7015_20260505_034128.txt`	Level 5 — BGP/Prefix
2026-05-05	`bgp_routing_history_AS7015_20260505_034008.txt`	Level 5 — BGP/Prefix
2026-05-05	`dns_AS7015_intl_20260505_020656.txt`	Level 3 — DNS/PTR check
2026-05-05	`prefixes_AS7015_20260505_010528.json`	Level 5 — BGP/Prefix
2026-05-05	`sample_ips_AS7015_20260505_010528.txt`	Level 5 — BGP/Prefix
2026-05-05	`whois_AS7015_intl_20260505.txt`	Level 4 — RDAP/WHOIS
2026-05-05	`whois_apnic_AS7015_20260505.txt`	Level 4 — RDAP/WHOIS
2026-05-05	`whois_arin_AS7015_20260505.txt`	Level 4 — RDAP/WHOIS
2026-05-08	`pdns_AS7015_20260508_174745.json`	Level 3 — Passive DNS
2026-05-05	`BLOCK 3–4 — BONUS– AS7015–8069.txt [shared: AS8069]`	Analyst synthesis
2026-05-05	`bgp_path_AS7015_intl_batch.txt`	Level 5 — BGP/Prefix

AS7029 — Windstream Communications LLC

Status: WINDSTREAM_RECLAIM | **Case ref:** CASE-010 | **Confidence tier:** R | **Evidence files:** 7

Prior CONTROL_LOST characterization retracted (CISA CORRECTION log UPDATE-002).
Not yet verified — correction to a prior draft (2026-08-18): an earlier version of this note claimed this association was "confirmed via live RDAP check, 2026-07-15." That claim was made

without a saved artifact to support it and has been retracted. The full `rdap-batch-20260506_022253.txt` batch (8 blocks: AS6478, AS7922, AS8069, AS7132, AS20115, AS5650, AS10913, AS7029) was checked directly and confirmed to contain only ASN-level registrant lookups — no query on `154.194.16.0/21` or any block-level record appears anywhere in it. The LARUS-SERVICE-MNT/Cloud Innovation Ltd association on `154.194.16.0/21` — the second half of Section 4.1's cross-ASN signature — remains documented only in `CISA-CORRECTION-AGGREGATE-VRF26-04-TPWXX.md` [NEW-001], with no independent block-level RDAP confirmation on file. `asn_source.json`'s silence on this block is a thin watchlist config, not a full analytic record, so it isn't treated as a contradiction — but this needs a direct RDAP query on `154.194.16.0/21`, likely via AFRINIC (Cloud Innovation Ltd is a Seychelles/AFRINIC secondary-market registrant, outside ARIN's authoritative region), before Section 4.1 can rely on it as a second confirmed instance. Not yet resolved either direction.

Date	File	Type
2026-05-05	`dns_AS7029_state_change_20260505_020107.txt`	Level 3 — DNS/PTR check
2026-05-05	`prefixes_AS7029_20260505_012337.json`	Level 5 — BGP/Prefix
2026-05-05	`prefixes_AS7029_20260505_015744.json`	Level 5 — BGP/Prefix
2026-05-05	`sample_ips_AS7029_20260505_012337.txt`	Level 5 — BGP/Prefix
2026-05-05	`sample_ips_AS7029_20260505_015744.txt`	Level 5 — BGP/Prefix
2026-05-08	`pdns_AS7029_20260508_192335.json`	Level 3 — Passive DNS
2026-05-08	`pdns_AS7029_20260508_193215.json`	Level 3 — Passive DNS

AS10913 — INTERNAP-BLK / Unitas Global (EarthLink successor)

Status: LEGITIMATE_SUCCESSOR | **Case ref:** CASE-010 | **Confidence tier:** R | **Evidence files:** 10

Formal retraction on file: CISA CORRECTION-002. Originally filed TRUE ZOMBIE (2026-05-02 supplemental); revised and retracted 2026-05-05 after Phase C confirmed Unitas Global as legitimate successor.

Date	File	Type
2026-05-03	`prefixes_AS10913_20260503_170109.json`	Level 5 — BGP/Prefix
2026-05-03	`sample_ips_AS10913_20260503_170109.txt`	Level 5 — BGP/Prefix
2026-05-05	`prefixes_AS10913_20260505_012337.json`	Level 5 — BGP/Prefix
2026-05-05	`prefixes_AS10913_20260505_015744.json`	Level 5 — BGP/Prefix
2026-05-05	`sample_ips_AS10913_20260505_012337.txt`	Level 5 — BGP/Prefix
2026-05-05	`sample_ips_AS10913_20260505_015744.txt`	Level 5 — BGP/Prefix
2026-05-05	`whois_arin_AS10913_20260505.txt`	Level 4 — RDAP/WHOIS
2026-05-08	`pdns_AS10913_20260508_192335.json`	Level 3 — Passive DNS
2026-05-08	`pdns_AS10913_20260508_193215.json`	Level 3 — Passive DNS
2026-05-05	`prefixes_AS10913_survived.txt`	Level 5 — BGP/Prefix

AS11427 — TWC-11427-TEXAS — Charter ARIN, BGP operator unknown

Status: THIRD_PARTY_CONTROL | **Case ref:** CASE-001 | **Confidence tier:** R | **Evidence files:** 8

Formal correction on file: CISA CORRECTION-001. Zone anchor status; Cloud Innovation Ltd / LARUS-SERVICE-MNT secondary-market pattern (see NEW-001, cross-referenced with AS7029).

Date	File	Type
2026-05-05	`dns_AS11427_state_change_20260505_020451.txt`	Level 3 — DNS/PTR check
2026-05-05	`prefixes_AS11427_20260505_012337.json`	Level 5 — BGP/Prefix
2026-05-05	`prefixes_AS11427_20260505_015744.json`	Level 5 — BGP/Prefix
2026-05-05	`sample_ips_AS11427_20260505_012337.txt`	Level 5 — BGP/Prefix
2026-05-05	`sample_ips_AS11427_20260505_015744.txt`	Level 5 — BGP/Prefix
2026-05-05	`whois_arin_156x_AS11427_20260505.txt`	Level 4 — RDAP/WHOIS
2026-05-05	`whois_arin_AS11427_20260505.txt`	Level 4 — RDAP/WHOIS
2026-05-08	`pdns_AS11427_20260508_174745.json`	Level 3 — Passive DNS

AS7046 — RFC2270-UUNET-CUSTOMER (Verizon Business / MCICS)

Status: ~~SINKHOLE_FEDERAL~~ → ~~UNREMEDIATED_VULNERABLE~~ → **NORMALLY OPERATED — reclassified 2026-08-25; malicious domain independently found in customer-aggregation space (see 5.3)** | **Case ref:** CASE-005 (WorldCom/MCI/UUNET lineage) | **Confidence tier:** R (bybanking.com finding only — see note) | **Evidence files:** 15

Reclassified 2026-08-25, on round-1 peer review + direct evidence recheck. Two prior labels — SINKHOLE_FEDERAL, then UNREMEDIATED_VULNERABLE — both assumed AS7046 was dormant or unstewarded federal space. Two pieces of evidence checked this pass do not support that: (1) AS7046's registration, `RFC2270-UUNET-CUSTOMER`, describes an ordinary shared-ASN function for a provider's single-homed customers — continuous full visibility is the expected state for this ASN type, not an anomaly. (2) A fresh RIPEstat upstream-neighbor query (2026-08-25, window matched to the existing AS7015 reference pull) found three of AS7046's five upstream peers are themselves Verizon Business/MCICS-registered sibling ASNs, with AS701 — Verizon's own UUNET backbone — as the dominant relationship by a wide margin (connectivity power 6752 against a next-highest of 278). This is what a normally operated carrier customer-aggregation ASN's upstream table looks like, not what a third-party-controlled one

looks like. The "reoccupied twice" narrative built on a "disruption" that Section 4.4 separately retracted — no dark window was ever confirmed for this ASN, so there is no gap for the space to have been "reoccupied" from. What is retained, because it does not depend on any of the retracted framing: `bybanking.com`, a domain independently flagged as malicious in February 2026, was found resolving into two of AS7046's announced blocks, two months apart, both independently confirmed as genuinely announced by this ASN. That finding is reported in full below and in Section 5.3.

RDAP originas data (reframed, per peer review P1-3). Five IPv6 blocks — `WIRE-V6`, `TERRENAP-V6`, `CFTC-NETWORK`, `DOLNET`, and `CMMS-IPV6` (identified in a later re-check, 2026-07-15; its registrant name is consistent with, but not independently confirmed as, the Centers for Medicare & Medicaid Services) — all return `originas: []` on RDAP, re-confirmed 2026-07-15. On round-1 peer review, this field was treated too strongly in the prior draft: an empty `originas` is RDAP's optional/default state, not a routing-authorization mechanism — RPKI ROAs and IRR objects are the actual authoritative record. RPKI validation checked directly against three of the five blocks (2026-08-25) returned `status: unknown` (no covering ROA published) for all three — indeterminate, not `invalid` (which would support the original claim) and not `valid` (which would refute it). TERRENAP-V6's actual announced prefix was identified (`2001:4868:207::/48`, one of six /48s AS7046 announces under its parent /32 — itself a pattern consistent with normal customer-block allocation) but its RPKI check has not yet completed; CMMS-IPV6 has not yet been checked. This is logged as in-progress, not resolved either direction.

Corroborated by the technical POC (OA12-ARIN) remaining unvalidated by ARIN since 2022-11-02, confirmed unchanged as of 2026-07-15 — an administrative gap consistent with the RFC 2270 customer-aggregation reading (Section 4.3) and not, on its own, evidence of unauthorized control.

Cross-ASN claim ruled out. A prior registry note suggested the CFTC-NETWORK block (`2620:0:250::/48`) also appeared in AS11427. Direct RIPEstat check of AS11427's full IPv6 prefix list (2026-07-14) shows this is **not the case** — the two ASNs' IPv6 space is entirely disjoint. This does not go into Section 4.1's cross-ASN pattern discussion; it was checked and did not hold up.

External corroboration of carrier identity (added 2026-07-30). Nemmi et al. (2021), independent of this investigation, document AS7046 in an unrelated case study (Section 6.4, "Unallocated ASNs used internally leak to the global Internet"): an unallocated ASN (AS290012147) announced a covered /24 for over two years (2015–2017), with the observed AS path forming the triplet `{AS290012147, AS7046, AS701}`. The authors state both AS701 and

AS7046 were held by Verizon at the time, and attribute the leak to an internal Verizon misconfiguration — not third-party occupation. This predates this investigation's evidence by roughly a decade and is now read differently than in the prior draft: it is early, independent, external confirmation of exactly what the 2026-08-25 upstream-neighbor check also found — **Verizon has operated AS7046 continuously, including at least a decade before this investigation began.** It supports Section 4.3's reclassification, not the paper's original stewardship-gap framing.

bybanking.com — two independent blocks, two months apart. Tier 3 pDNS (2026-06-16): subdomain `9ve2e267.bybanking.com` resolves to `161.162.17.104` in `161.162.17.0/24`. A second pDNS run (2026-07-15): `ns-5whj.bybanking.com` resolves to `198.57.13.170` in `198.57.13.0/24` — a different subdomain, IP, and /24 entirely. Both blocks independently confirmed as genuinely announced by AS7046 via direct RIPEstat prefix-list query, not inferred from the pDNS tool's internal sampling. Two independently-confirmed hosting blocks two months apart is a persistent pattern, not a single stale record.

Falcon Sandbox — six analyses now. The Feb 9, 2026 report (analysis `6989f42c...`, third-party/pre-existing, found via search) shows bybanking.com resolving to 148.17.131.206 (US), threat score 45/100, 1 domain/3 hosts contacted, TTL-5 fast-flux. A second analysis (`6a31af53...`) was submitted 2026-06-16 by this investigation directly — **a deliberate exception to the standing sandbox-resubmission protocol**, made to answer a specific question the Feb report couldn't: whether the block showed signs of reactivating, and if so, in what form (continued sinkhole/honeypot use vs. genuine criminal reoccupation). Results differed meaningfully: bybanking.com resolved to 45.145.86.142 (United Kingdom, not the US), 11 domains/18 hosts contacted, active HTTP traffic and Suricata alerts present, and a different OS/browser sandbox environment (Windows 11/Chrome vs. Windows 10/Edge).

Two further analyses were submitted 2026-07-15, same investigation account, same deliberate-exception rationale: a Windows 11 run (`6a56f6183bcc...`, 02:53 UTC) with bybanking.com resolving to 175.232.34.31 (**South Korea**), and a Windows 10 run (`6a56fdb39723...`, 03:25 UTC, 32 minutes later) resolving to 101.98.55.5 (**New Zealand**) — a different country in each of four checks now (US → UK → South Korea → New Zealand), the tightest rotation window observed to date. Both July reports carry Hybrid Analysis's own automated warning that the verdict ("no specific threat") does not match other analyses of the same file hash and may be outdated — notable because both July runs detected *more* indicators than the earlier ones (16–17, plus a new Suricata alert category) while receiving a *lower* threat classification than the Feb/Jun

"suspicious" verdicts. This inconsistency is recorded here as observed, not resolved; it is not this paper's place to arbitrate between Hybrid Analysis's own scoring runs.

Two more analyses were submitted 2026-07-25, 35 seconds apart, both crossing into **"malicious"** verdict territory for the first time (prior verdicts topped out at "suspicious"): a Windows 11 run (`6a640572395a8786460e0c4c...`, 00:38:11 UTC, threat score 76/100) resolving to 123.150.3.39 (**China**), and a Windows 10 run (`6a64054fcf58877fc3076b10...`, 00:37:36 UTC, threat score 70/100) resolving to 145.74.110.172 (**Netherlands**). Both carry a new "Malicious domain detected" indicator and cookie-theft behavior ("Attempts to retrieve cookies from browser memory," "Able to access web session cookie") not present in earlier runs — a genuine behavioral escalation, independent of the threat-score trend, which is also consistent with the general pattern of reputation-platform scores climbing as a known-bad domain accumulates detection history rather than necessarily reflecting a real-time change in the infrastructure itself.

The China-resolving block was directly checked against AS7046 and is not part of it. Live RIPEstat query (2026-07-26) against AS7046's full IPv4 prefix list confirms `123.150.3.39` does not fall within any AS7046-announced block. This is the first confirmed instance of `bybanking.com` resolving entirely outside AS7046's address space, and confirms the *domain* has moved off this ASN's space. It has no bearing on Section 4.3's reclassification of the ASN itself — that assessment rests on the upstream-neighbor and RFC 2270 evidence, not on the domain's current resolution pattern. The Netherlands-resolving IP (`145.74.110.172`) has not yet been checked against AS7046's current prefix list.

On attribution: HA's country tagging for the China- and Netherlands-resolving IPs establishes hosting location only, not operator identity. Leased, compromised, or bulletproof-hosting infrastructure in either location would produce the same geolocation signal regardless of who is actually operating the campaign. This paper does not assert an operator location beyond what is directly supported.

This is disclosed here for transparency: all five post-Feb submissions are investigation-generated evidence, not discovered third-party data, and all post-date this investigation's own Tier R sinkhole confirmation (2026-05-27).

Current routing state (re-confirmed 2026-07-14/15): 220 IPv4 prefixes, 24 IPv6 prefixes, 100% RIS visibility (326/326 IPv4 peers, 321/321 IPv6 peers), last seen 2026-07-14T16:00:00. Not dark, not dormant — fully visible in global BGP routing as of this writing.

What this does not establish (per the source finding's own limits, carried forward under the actor-agnostic framing in Section 2.3): why `bybanking.com` specifically surfaced in this ASN's customer space; the identity of the threat actors whose callbacks were being captured, if the sandbox-observed redirection behavior was deliberate; or whether the Hong Kong contact (`63.222.23.49`, Feb report) is part of the same operation. The "federal capture point" and "sinkhole" framing in the original draft assumed a stewardship gap that Section 4.3 has since retracted; no such framing is asserted in this revision.

Reporting status — corrected. The original source finding claimed AS7046 was "reported to CISA + FBI 2026-05-02." Direct text search of the actual filed 2026-05-02 CISA supplemental and both versions of the correction aggregate log confirms **zero mentions of AS7046 in any of them** — and the claim is chronologically impossible regardless, since AS7046 wasn't a named candidate in this investigation's own batch planning until after that date, and its Tier R confirmation didn't occur until 2026-05-27. The finding was actually transmitted via IC3 on **2026-07-16**.

Reporting delay — flagged as a process concern, not minimized. The bybanking.com C2 finding was discovered 2026-06-16 and not actually reported until 2026-07-16 — **exactly 30 days.** The proximate cause is on record: the 2026-06-16 finding document's own "Report Status" section stated AS7046 had already been reported on 2026-05-02 and that "no additional disclosure action is required." That belief was false, but nothing tested it until this paper's drafting process independently swept the actual CISA filings weeks later and found no record of it. For an active banking-malware C2 domain, a documentation error that goes unchecked for 30 days is not a minor bookkeeping issue — it is 30 days the domain continued operating unflagged to any external party who could act on it. This is logged here as a concrete illustration of the broader methodological point already made elsewhere in this paper (Section 2.5's "cleared findings are retained" principle, and the AS10913/AS6181 cases): an unverified claim about disclosure status is itself a finding that needs the same evidentiary discipline as any other, and this is the one case in this investigation where that discipline was applied too late to prevent real-world consequence.

Date	File	Type
2026-02-09	Falcon Sandbox report, `bybanking-february-2026.pdf` (analysis `6989f42c...`)	Third-party OSINT — pre-existing, found via search
2026-05-27	RDAP originas batch — `7046--confirmed--FF.txt` (raw RDAP queries, primary source)	Level 4 — RDAP/WHOIS
2026-06-16	`BIV-ANO-2026-06-16_AS7046-PDNS-BYBANKING.md`	Level 3 — Passive DNS + analyst synthesis
2026-06-16	Falcon Sandbox report, `bybanking-june-2026.pdf` (analysis `6a31af53...`)	**Investigation-submitted** — deliberate reactivation check, not third-party OSINT
2026-06-16	`BIV-PND-2026-06-16_SESSION-PAUSE-STATE.md`	Session state / procedural record
2026-07-15	Second pDNS finding — `198.57.13.0/24`, `ns-5whj.bybanking.com`	Level 3 — Passive DNS
2026-07-14/15	Live re-confirmation — RDAP (5 blocks), RIPEstat routing-status, ASN-level RDAP, AS11427 cross-check	Level 4/5 — RDAP + BGP, current as of filing
2026-07-15	Falcon Sandbox report, `bybanking-july-2026-win11.pdf` (analysis `6a56f6183bcc...`, 02:53 UTC)	**Investigation-submitted** — reactivation check
2026-07-15	Falcon Sandbox report, `bybanking-july-2026-win10.pdf` (analysis `6a56fdb39723...`, 03:25 UTC)	**Investigation-submitted** — reactivation check
2026-07-15	`CISA-FBI-INITIAL-AS7046-BYBANKING-2026-07-15.txt`	Drafted disclosure filing, superseded the earlier `CISA-SUPPLEMENTAL-...` draft.

Date	File	Type
2026-07-16	IC3 filing confirmation, Submission ID `1ac64da023d24387bc4e6dd811b8c456`	**Transmitted.** 30 days after the underlying finding (2026-06-16). See reporting-delay note above.
2026-07-25	Falcon Sandbox report, `HA-072726-bybanking-dot-com-W11.pdf` (analysis `6a640572395a8786460e0c4c`, 00:38:11 UTC)	**Investigation-submitted** — first "malicious" verdict (76/100), resolved to China
2026-07-25	Falcon Sandbox report, `HA-072726-bybanking-dot-com-W10.pdf` (analysis `6a64054fcf58877fc3076b10`, 00:37:36 UTC)	**Investigation-submitted** — 70/100 malicious, resolved to Netherlands
2026-07-26	Live RIPEstat check — `123.150.3.39` confirmed **not** in AS7046's announced IPv4 space	Level 5 — BGP/Prefix, current as of filing
2026-06-18	`SNAP-BASELINE-20260618.md`	Level 5 — BGP/Prefix (change-detection baseline, includes AS6128 cross-reference)

8.1c Summarized Evidence — Non-Load-Bearing ASNs

The following ASNs are cleared/stable with no open questions; most are not individually discussed in the narrative beyond their appearance in Table 4.1 (Section 4.2) or as baseline, comparison, or control entries. Full per-file evidence tables have been condensed to one row each; raw filenames and per-file hashes remain in `SHADOW_MARKET_FILE_HASHES.txt` regardless of this summarization.

ASN	Entity	Status	Case ref	Files	Role / Note
AS209	CenturyLink/Lumen — Qwest/Embarq successor	LEGITIMATE_SUCCESSOR	CASE-007	4	Baseline
AS701	UUNET / Verizon Business — MCI successor	LEGITIMATE_SUCCESSOR	CASE-005	10	Comparison/control (pair with AS3549). *Handoff ref table flags a "CISA correct UPDATE-003" tie for this A not present in this paper's text or in* `SHADOW_MARKET_FILE_HASHE` *Unverified; flagged for ana confirmation, not asserted*
AS702	UUNET-AS702 / Verizon Business legacy	LEGITIMATE_SUCCESSOR	CASE-005	2	Comparison/control
AS2686	ATGS-MMD-AS — AT&T Enterprises LLC	MISATTRIBUTION → LEGITIMATE_SUCCESSOR	CASE-007	1	Comparison/control; prior working assumption (Spri FL/Embarq) corrected via RDAP+RIPEstat
AS3549	Lumen / Level 3 — Global Crossing successor	LEGITIMATE_SUCCESSOR	CASE-004	10	Paired run with AS701. *Sar unverified UPDATE-003 reference as AS701 above note.*
AS5650	FRONTIER-FRTR — Frontier Communications	MISATTRIBUTION	CASE-007	1	Comparison/control; prior working assumption (Emb Corp) corrected

ASN	Entity	Status	Case ref	Files	Role / Note
AS6128	Cablevision Systems (Altice retained)	RETENTION_ANOMALY	CASE-009	4	Baseline
AS6478	TCI/@Home (collapsed 2001, properly retired)	CLEAN	CASE-003	4	Baseline
AS7132	SBIS-AS / SBC Internet Services / Ameritech backbone	CLEAN	CASE-006	1	Baseline
AS7922	COMCAST-7922 (post-TCI production ASN)	CLEAN	CASE-002/003	3	Baseline
AS8069	Microsoft Corp — misattributed to Ameritech	MISATTRIBUTION / **ACTIVE_MONITOR? — unresolved source conflict**	CASE-006	6	Cited in Table 4.1 (Section as its own disposition row status conflict, not cleare independently resolved. **C item, carried forward, no silently resolved:** `ZOMBIE-REGISTRY.db` shows escala to ACTIVE_MONITOR (20 12); `asn_source.json` (documented source of tr shows MISATTRIBUTION, 2026-05-06, and has no ACTIVE_MONITOR value schema. PeeringDB confir

ASN	Entity	Status	Case ref	Files	Role / Note
					AS8069 as Microsoft Azur Routing Preference regar of which status label is cu
AS10796	TWC-10796-MIDWEST (Charter retained, clean)	CLEAN	CASE-008	2	Baseline
AS11426	TWC-11426-CAROLINAS (Charter dual-ASN retention)	RETENTION_ANOMALY	CASE-001	3	Baseline
AS14905	CENTURYLINK-LEGACY-EMBARQ-VACHVL	LEGITIMATE_SUCCESSOR	CASE-007	1	Comparison/control
AS20115	Charter/Spectrum (production ASN)	CLEAN	CASE-001	1	Baseline
AS33363	BHN-33363 — attribution conflict (Adelphia vs. BHN)	PENDING_VERIFICATION → RETENTION_ANOMALY (confirmed 2026-05-07)	CASE-002	6	Corrected, not cited in Se 4. Live recheck (2026-07- registrant/status unchang prefix count 494→436 (12 decline since baseline), ca open — no baseline total- figure on file to distinguis genuine shrinkage from ro aggregation. Logged CHG_DETECTED, not reso either direction.

ASN	Entity	Status	Case ref	Files	Role / Note
AS36727	Insight Communications (post-acquisition clean)	CLEAN	CASE-008	3	Baseline
AS54396	Nuance Communications (small ASN, misattributed to Altice's cable ASN)	CLEAN → MISATTRIBUTION	CASE-009	1	Corrected, not cited in Se 4. ARIN name is NUANCE MOBILITY, 1 active prefix; AS6128 remains Altice's a cable ASN for CASE-009.

Subtotal, summarized ASNs: 18 ASNs, 63 evidence files.

8.2 Multi-ASN / Batch Evidence

Cull review: reviewed during the 2026-07-29 evidence cull and kept as-is — already condensed to type/count/date-range on a prior pass; no further trimming warranted.

Files not attributable to a single ASN — BGP watchlist monitor runs, batch DNS/pDNS sweeps, and multi-ASN RDAP/registration analyses. Cross-referenced under each relevant ASN above where applicable (e.g., the AS701/AS3549 RDAP analysis and the AS7015/AS8069 synthesis document each appear once here in aggregate and once under their respective ASN sections above). Summarized by type rather than listed individually; raw filenames and per-file hashes remain in `SHADOW_MARKET_FILE_HASHES.txt`.

Type of Data Run	Number of Runs	Date Range
BGP watchlist monitor (`zombie_report`)	42	2026-05-03 – 2026-05-20
DNS/PTR check (`dns_check_batch`)	12	2026-05-03 – 2026-05-04
pDNS run log (`pdns_run`)	11	2026-05-08 – 2026-05-09
pDNS summary (`pdns_summary`)	11	2026-05-08 – 2026-05-09
RDAP/WHOIS (multi-ASN)	6	2026-05-05 – 2026-05-06
Procedural/command log	4 (incl. `5-4-26-zombie-hunter-TerminalOutput.txt`, renamed from `Terminal Saved Output.txt`; `terminal-may5.txt`)	2026-05-04 – 2026-05-05
Other (incl. `setiii-rdap-arin.txt`)	3	2026-05-03 – 2026-05-06
Analyst synthesis, multi-ASN (`BLOCK 3-4`)	1	2026-05-05
BGP/Prefix, multi-ASN	1	2026-05-05
Total, batch/multi-ASN evidence	**91**	**2026-05-03 – 2026-05-20**

8.3 Supporting Case Documents (Session-Provided, Not Per-ASN Evidence)

Working documents used to reconcile the evidence base and resolve the AS6181/AS2686

corrections. Retained for chain-of-custody completeness; not attributable to a single ASN.

Date	File	Role
2026-05-02	`CISA-SUPPLEMENTAL-ZOMBIE-BGP-2026-05-02.txt`	The actual filed CISA supplemental report. Confirmed AS6181 was never included in this filing (swept for "6181", "AS702", "5650", "14905" — no genuine matches).
2026-05-02	`phase_a_candidates_20260502_011511.csv`	Phase A national survey scoring output; source of the original (later corrected) AS6181/Insight zombie-BGP flag.
2026-05-08	`PDNS-BATCH-QUEUE.txt`	Batch run plan confirming AS702/AS2686/AS5650/AS14905 were planned, in-scope VRF#26-04-TPWXX candidates (Batches C–E), not cross-case artifacts.
2026-05-07 to 2026-05-19	`BACKBONE-INVESTIGATION-LOG-v2.md`	Working investigation log; source for registry expansion (I-027, 20→23 ASNs) and the AS7015 post-05-19 status question flagged in the AS7015 entry above.