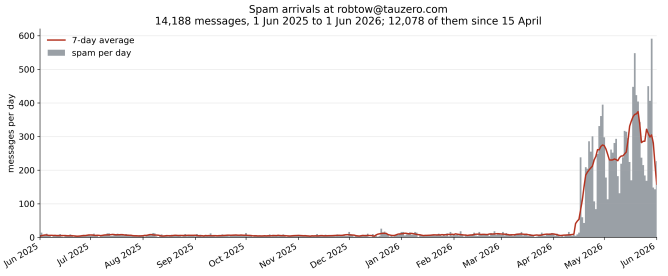
Banker's Hours: Who Goes There?

Rob Tow

Nova Lux, New Mexico, USA, Sol III

4 June 2026



Spam arriving at robtow@tauzero.com, one bar to the day, June 2025 through May 2026: a flat baseline near zero for ten and a half months, then a cliff in the middle of April 2026 to two and three hundred a day, holding through May.

> *A 40-fold spam flood arrives in my self-hosted mailbox in one week of April 2026 and does not recede. Read as a control loop: the traffic keeps North American banker's hours though its machines are rented worldwide; the domains are dollar burners struck once and dropped; nearly half the messages hide AI-written prose to poison the filter; and a leaked generator prompt confirms the design —hold the con fixed, vary the wrapper without limit. Why chasing domains is a losing loop, why the walled gardens win, why no one goes to prison for this now, and why I still run my own iron.*

14,188 pieces of spam reached me in the year to this June, but the figure that matters is not the year's; it is the final six weeks'.[1] For ten

[1] **What counts as spam here.** The corpus is my Spam folder, everything my host and its filters set aside over the trailing year, parsed from a frozen, hashed snapshot of the mbox rather than from live mail that keeps changing under one's hands. It

and a half months the count was beneath notice, a median of 7 a day, the ordinary tax on an open port. Then, in one week in the middle of April, the rate stepped to better than 290 on weekdays and held there: 12,078 of the year's pieces, five in every six, arrived after that step. The graph above is the whole year, one bar to the day; the cliff needs no caption.

I keep my own mail server, on a bare shell account on an old and bunkered Linux host. This is informed by what I practiced in the Cold War working with and building radar and electronic warfare systems that publicly lied about state and possibility. Old habits about verification hold, so I measured before I theorized, and treated the thing as what it is: a control loop, a filter and an adversary coupled, each adapting to the other and leaving its tracks in the headers. A 40-fold jump that arrives in a week and does not wander afterward is not weather. This is a change in climate, and a change in climate has a cause one can name precisely instead of cursing in the abstract. The cause is not peculiar to spam. It is the same arithmetic now closing the open internet, and it fixes the boundary of what a small operator can still do about it.

The first thing the traffic gives up, when you sort it by the clock, is a rhythm so regular it might have been punched on a time card. Monday through Thursday the flood runs between 278 and 298 pieces a day; Friday it peaks at 348; then it stands down to 135 on Saturday and 131 on Sunday. Sorted instead by the hour, the same hand shows itself: the volume bottoms near 2 percent of the daily total between four and nine in the morning, Universal Time, and

---

is not an adjudicated set, and a careful reader should weigh it both ways. The "From"line is forged as freely as the "Date,"so the apparent senders include my own domain and Amazon and the like, wearing names they never owned; that is exactly why I read the relay chain and the pitch and never the "From."A little real mail lands in the folder by mistake and is fished back out as I notice it, a small contamination of the quiet months that touches none of the hidden-ballast count.

crests at 8.6 percent at seventeen hundred hours, one o'clock in the afternoon on the American East Coast and eleven in the morning where I sit in New Mexico. Read in Eastern time, which is where the continent keeps its commercial center of gravity even though I sit a zone west of it, the flood wakes at nine in the morning, peaks at one in the afternoon, and sleeps through the American night. A five-to-one swing between the noon flood and the small-hours trickle is not the work of a machine grinding around the clock; a machine grinding around the clock draws a flat line. This is something keeping a calendar, and keeping it on a North American working week.[2]

My first inference was wrong, and the manner of its wrongness is a most useful thing in the investigation. A rhythm that runs on the working week and the working day is the duty cycle of compromised office machines: desktops powered up when the worker arrives, infected and relaying through the day, switched off at night and over the weekend when the office goes dark. That was my model, and it was a satisfying one; I had even drafted a line about Windows as a wonderful host for parasitism. But a model is only a hypothesis about ground truth, and ground truth in this trade lives in the email headers. So I went to the headers, and they declined to confirm me. I was wrong, and knowing that recreated my understanding. As a scientist and engineer I like finding out that I'm wrong about something, because then I am *improved*.

Every message carries, in its headers, the fingerprints of the ma-

[2] **The clock springs forward.** If the crew keeps Eastern wall-clock hours, daylight saving should leave a mark: the peak ought to fall one Universal-Time hour later in winter than in summer, and to line up when read in New York time. It does, faintly. In the quiet months before the flood the arrivals crest at sixteen hundred UTC under standard time and fifteen hundred under daylight time, both near eleven in the morning on the East Coast. I will not lean on it; the baseline is thin and mixed, and shows only that the American senders in my spam keep daylight saving like everyone else, while the flood itself fell wholly within daylight time and cannot be made to testify. A partial confirmation, offered as one.

chines that handled it.[3] I pulled the network addresses of sixty of the senders, spread from the heaviest to the rarest, and looked up who owns them. Not one is a home or a cubicle. There is no Comcast, no Spectrum, no consumer carrier of the kind a botnet of infected desktops would ride. What there is instead falls into two camps: hijacked or rented marketing platforms, Salesforce and SendGrid and Amazon and Acoustic, the very email services that legitimate businesses use to send you their newsletters; and rented datacenter and virtual-server space scattered across a dozen countries, the United States and India and Italy and Tunisia and Vietnam and the Seychelles.[4] These are not the conscripted desktops of my tidy theory. They are always-on machines, deliberately dispersed, rented by the hour.

Which leaves the calendar demanding a new explanation, and the new explanation is better than the one it unseated. If the machines never sleep, the workday rhythm cannot be theirs; it must belong to the hands that drive them. The infrastructure is global and tireless, but the operators who load the campaigns and press the button keep office hours, on a North American week, and rest like any wage-

[3] **The honest clock.** Every server that touches a message stamps it with a "Received"header bearing that server's own clock; the topmost such header is the final receiver, here my own host, and its time is the true moment of arrival. The sender's "Date:"header, by contrast, is decoration, and on fraudulent mail it is routinely false, so to time arrivals one reads the machine that caught each letter, never the machine that claimed to send it. The figures throughout are parsed straight from the mbox my host files, using the timestamps its own filter applied.

[4] **Sixty addresses.** I sampled sixty source addresses from the flood, weighted from the heaviest senders down into the long tail, and resolved each through WHOIS. The owners cluster as email-service providers (Salesforce and ExactTarget, SendGrid, Amazon SES, Acoustic) and as rented datacenter ranges in the United States, India, Italy, Tunisia, Vietnam, the Seychelles, and elsewhere; not one is a residential consumer ISP. The honest caveat: these are the addresses in each message's relay chain, the sending and transiting infrastructure, not necessarily an ultimate human origin. The robust conclusion is the negative one. No desktops.

earner on Sunday. The clock and the headers, in other words, disagree: the clock tells me where the crew works, and the headers tell me where the guns are rented, and the two addresses are nowhere near each other. That disagreement is not a defect in the data; it is the finding. Capability has gone global and rented by the hour, while intent still keeps a single, parochial, nine-to-five calendar. I would never have seen it had I been unwilling to throw away an explanation I liked. Correction in the face of evidence is not a humiliation to be hurried past; it is the whole of epistemic hygiene, and the only thing that separates a measurement from a flattering story about oneself.

Having lost one theory, I handled the next with more care, and that next concerned the domains. My banal first guess had been that my address was simply sold onto a mailing list. The domains say otherwise, and they say it loudly. The 12,078 pieces of the flood arrived from 3,742 distinct registered domains, an average of barely three apiece, and three-quarters of those domains were alive, by the evidence of their own traffic, for less than a single day before going silent forever.[5] Many were registered the very morning they wrote to me and abandoned by nightfall. A mailing list is a durable asset, husbanded and reused; these are not lists, they are matches, struck once and dropped. And their names give the game away. cuddlymarshrr.pro, sunrisebeacon.bond, cedartrail92.net, fieldstonepanel.pro, roomsrural.garden: pronounceable pseudo-brands, assembled adjective-and-noun and padded with a random syllable or a pair of digits until the registrar found a string nobody had claimed, parked on the bar-

[5] **The burner census.** The flood resolved to 3,742 registered domains, counted at the level of the registered name rather than the host, a mean of 3.2 messages apiece. Better than three-quarters, 76 percent, showed a first-to-last span under twenty-four hours, and 84 percent within a week. The novelty extensions (.bond, .garden, .shop, .lat, .world and their kin) ran 91 to 100 percent single-day burners; even among the .com names, two-thirds burned within a day.

gain extensions where a fresh name costs a dollar or two. No clerk hand-named three thousand of these in a morning, and no copywriter hand-wrote the 6,308 distinct subject lines that came with them. Machines did both. This is what artificial intelligence looks like when it is set to work inside the walls of the house of email: not a chatbot to amuse you, but a foundry stamping out disguises faster than any human institution can tear them off. Burning down the house.

The economics are the engine, and they are worth understanding, because they explain why this arrived now and not five years ago. A name on one of these discount extensions on the latest top level domains runs a dollar or two for the first year and rather more to renew; but a burner is never renewed, because it is dead by lunch, so only the rock-bottom introductory price ever applies, and the renewal fee that disciplines an honest registrant into keeping a single durable name is simply never paid.[6] The registries that sell the names are willing accessories to the arithmetic: the most-abused of these extensions are among the fastest-growing on the internet, their registrations up well over a hundred percent in a single year, while their only conspicuous product is fraud.[7] When the marginal cost of a credible disposable identity falls below the cost of the postage it carries, identity stops being a constraint, and every defense built on the

[6] **A dollar a name.** First-year registration on the discount extensions, as listed by a major registrar at the time of writing: .shop about $1.28, .bond between $1.60 and $2.69, .lat and .click about $1.80, with some registrars advertising names from $0.88. A United States first-class stamp is about $0.78. See namecheap.com/domains/registration/gtld/bond/ and the parallel pages for .lat and .shop.

[7] **The worst neighborhoods.** Spamhaus tracks a "badness" ratio, abusive domains as a fraction of all domains it observes, broken out by top-level domain; the cheap, high-churn extensions dominate the list, and registrations on the worst of them (.sbs and .bond among them) have lately grown 172 and 148 percent year over year. See spamhaus.org, "Spamhaus Presents: The World's Worst Top Level Domains."

durability of identity collapses with it.

Not every domain is newborn, and the exceptions are instructive. A minority are aged and respectable dot-coms with a decade of innocent history behind them: a tire shop, a door company outside Roswell, the sort of small concern that registered a name once and forgot it. These were either hijacked outright or bought on the secondary market, and they are prized for the one quality a freshly minted name cannot counterfeit, which is age, the very thing a reputation filter is built to reward. So the supply is not a single trick but a portfolio: same-day disposables for raw volume, warmed names aged a few weeks to slip past the new-domain filters, and stolen old names for the messages that must look most respectable. The con buys honesty when it needs it and prints disposability when it does not.

Stand back from the particular tricks and one principle is doing all the work: every input that used to be scarce, and therefore a constraint, has gone *cheap, fast, and out of control.* I have watched this happen before in another domain, that of personal publishing, and anciently helped it along. In the 1980s the means of producing the printed word fell into private hands, the laser printer and the photocopier and the desktop machine, and a thousand zines bloomed that no gatekeeper had licensed; I was at Xerox PARC while some of that machinery was being built, and I counted the democratization a good thing. The same collapse has now reached the production of fraud. Identity costs a dollar and is minted by the hundred thousand, the registrars selling registration in bulk through an interface and supplying the name-generator themselves; one operator was lately found to have spent a little over a million dollars to register half a million algorithmic domains in a single year.[8] Content is free

[8] **Identity by the hundred thousand.** Interisle Consulting's *Cybercrime Supply Chain 2025* counts more than 7.3 million cybercrime domains registered in bulk,

and instant, the foundry already described. The sending is rented by the hour on someone else's reputable machine. The phrase I have used for forty years for what the press in private hands did to the gatekeepers of print now serves, without alteration, for what the language model in private hands does to the filter: exactly cheap, fast, and out of control.

The foundry does not stop at the disguise on the envelope; it has turned, lately, on the mind of the filter itself. Open one of these letters and read not what it shows to the human gaze but what it hides, in the markup where no human eye is meant to fall (open a special edit window to do this), and you find a paragraph of placid, fluent, entirely innocent prose: someone agreeing to meet a little earlier on Thursday, someone who meant to reply sooner but let the afternoon get away.[9] It is not the pitch. It has nothing to do with the pitch. It is written to be read by the machine and not the man, ballast whose one purpose is to drag a traditional Bayesian statistical filter, which learns what honest mail looks like from the words inside it, toward the verdict that this letter is a friend. The trick is old; spammers have larded their messages with innocuous words since John Graham-Cumming named the attack at the 2004 spam conference, when the poison was visible word salad that no reader would

---

bulk registration up 177 percent in a year, and one operator who spent better than a million dollars to register some 500,000 algorithmically generated domains in 2024; the random-looking strings betray a registrar's own name-generator at work. The trade sells identity by the truckload to customers it knows mean to keep none of it, and counts the receipts. See interisle.net.

[9] **Steganography, honorably and otherwise.** Hiding data inside an innocent-looking picture or document is an old craft; I spent years at PARC doing it on purpose, packing kilobits invisibly into the gray squares on a printed page (see "DataGlyph,"https://www.tauzero.com/Rob_Tow/DataGlyph.html). The technique is honorable. Stuffing a paragraph of fabricated friendly chatter into an email to fool its reader's filter is the same craft in the hands of a mugger.

mistake for speech.[10] What is new is that the salad, thanks to AI, is literate. I measured it against my own mailbox: of the flood's 12,078 messages, 5,824, very nearly half, carry such a hidden ballast, a median of 177 words apiece, and when I tested whether the buried text was random or real, ninety-eight in a hundred read as coherent English.[11] The word-salad of 2004 did not get cruder. It got grammar, and a place to hide. It apes humanity.

This is The Thing of the old film, and the question the title asks: *who goes there?* The hidden paragraph is an imitation built to be indistinguishable from the genuine article, innocent correspondence manufactured to fill the filter's sense of the normal with friends who were never there. I have worked on such a thing myself, in another war. At Northrop in 1979 I worked on a machine that generated coherent false radar returns, convincing aircraft with convincing Doppler, enough to populate a SAM operator's scope with a squadron that did not exist.[12] This is the same maneuver, made in language instead

[10] **Bayesian poisoning.** Lacing a message with innocuous or "good" words to drag a statistical (Bayesian) filter below its threshold was demonstrated by John Graham-Cumming at the 2004 MIT Spam Conference. The original form was visible "word salad," clumsy strings of dictionary terms; the form measured here is coherent generated prose, hidden in the markup. The attack is twenty years old; only the prose is new. See en.wikipedia.org, "Bayesian poisoning."

[11] **The hidden-ballast measurement.** Parsed from the frozen snapshot over the flood window. For each message I parsed the HTML, separated the text hidden by CSS or markup from the visible text, counted the hidden words, and tested whether their vocabulary was foreign to the visible pitch: 5,824 of the flood's 12,078 messages carried fifty or more hidden words whose vocabulary was largely foreign to the pitch, a median of 177 words apiece. Coherence was scored by the function-word ratio of the hidden text, which runs high in real English and very low in a "good-word" salad; 98.1 percent scored as coherent prose, a reading confirmed by hand against a random sample of 361 messages (95 percent confidence, plus or minus five percent). Of that hidden text, about 86 percent reads as fabricated contemporary personal email and a trace, well under a percent, as scraped public-domain prose.

[12] **The 1979 machine.** The radar-signal emulator I worked on at Northrop

of microwaves and aimed at a classifier instead of a radar, a coherent false return fired into the estimator. And it points, before one has argued the point, at the only test that ever told the Thing from the man: not an inventory of what the imitation looks like, which it can always counterfeit, but a reading of what it is for. A blood test. The one thing the imitation cannot fake is its *purpose.*

I would have left the matter there, an inference from the shape of the evidence, except that I did a deeper forensic dive and found the machine confessed. In a fraction of these messages the generator's own instructions to the AI had leaked into the output it was told to produce, the way a careless clerk leaves the brief stapled to the letter, and the prompt describes this essay better than I can.[13] The half that builds the visible letter orders the model to "create a new email variant that stays on-brief but not on-template," to "keep the same brand and same core offer, make the email feel like the same campaign family, not a different product," while it randomizes "tagline phrasing, layout density, headline construction, CTA wording . . . section order," and to make each run "a fresh concept, not a lightly edited duplicate." This is what I learned the slow CSI way, set down as a work order: hold the con fixed, vary the wrapper with-

generated coherent false returns, with Doppler, to fill a hostile scope with aircraft that were not there; I have told that story in "Radar Love" (https://www.tauzero.com/Rob_Tow/essays/radar-love.html). Then it was microwaves and an honest enemy; now it is prose, and a grifter selling counterfeit gift cards.

[13] **The leaked prompt.** A fraction of the messages carried, in their hidden text, the generator's own instructions, rendered into the output the way a model echoes its brief when told to "return only the HTML" and obeys imperfectly. The quotations are verbatim from those messages, in two modules: one governing the visible letter ("Core brief," "Run variance"), one governing the hidden ballast ("HARD RULES," "MAILER VARIATION TOKENS"). The same kit was caught spoofing Lowe's and Verizon with identical machinery, down to a parameterized "color temperature" and a literal run seed. Held in the frozen corpus; reproducible from it.

out limit. The half that builds the hidden ballast is blunter still. Its "hard rules"forbid an unsubscribe link, forbid a street address, forbid an HTML comment; they drop into every copy a random token that "makes every recipient's email fingerprint-unique at the inbox level"; they command it to "generate completely new content for every run, never reuse,"to write "natural, human-like, and conversational,"in "first person,"to mention nothing of "money, costs, pricing, or anything financial,"and, last, to "not reference or mention hidden text anywhere in the visible email content."Every property I had measured is there in the operator's own hand: the unique surface, the friendly register, the studied silence about the very thing the letter is selling, and the deliberate defeat of the shared-fingerprint filters on which the small operator's last hope depends. It is a checklist drawn up against every defense email ever grew.

This is a single hand, exposed with blood. Behind the flood is a small ecology rather than just the one foundry: one observably dominant and sophisticated kit, brand-agnostic, dressing the same machinery as Lowe's in one hour and Verizon the next; a fringe of lesser kits that speak its grammar in a different dialect, plainly forks or imitations of the one design; and a scatter of older, cruder operations, fake polls and survey-reward come-ons and supplement quackery, riding the same week.[14] The iron beneath them is rented cheap and global, datacenter blocks in the Asia-Pacific and Africa, a little Google Cloud, a little Amazon, all of it disposable. And here the

[14] **How many hands.** Forensic fingerprinting of the flood (leaked-prompt grammar, mailer strings, signing and Message-ID domains, sending blocks, and arrival cadence) collapses the bespoke artifacts to single digits or low dozens of distinct kits and operations, riding thousands of disposable domains and IPs: a small competitive trade of foundries, not one empire and not ten thousand lone spammers. The leaked-prompt templates and the bespoke mailer names are the closest thing to an author's hand; the disposable domains and rented IPs say nothing about how many actors. A signature is not a name; the operation is built to keep it that way.

oldest tool of attribution fails. For thirty years the broken English and the foreign idiom were how one guessed where a spammer sat; the language model now writes flawless American English (I found no "colour," no "theatre," no "honour") no matter whose hand is on the keyboard, and the accent is gone. The only origin the machine could not launder is behavioral. The work keeps banker's hours, on a North American week, whatever the rented box in Tunisia reports. The model erased the tell that lived in the words; the one that lives in the calendar it could not reach.

Set the economics beside the infrastructure and the whole design resolves into one principle, and it is the principle that defeats every defense email grew up with. Those defenses assumed scarcity. They assumed a sender had to husband a name, a reputation, an address worth protecting, and they worked by remembering which names had misbehaved and refusing them. Block a domain under that regime and you have punished something the spammer valued. Block a burner and you have killed something already dead, on which he spent nothing he meant to keep. To chase the domains is to orient your entire apparatus on the one variable your adversary can change for free, which means you are forever one move behind him, learning each disguise exactly one day after it has ceased to matter. In the language of control this is a loop whose latency exceeds the rate at which its target moves; such a loop never reaches its setpoint, it only chases. John Boyd, who taught fighter pilots how to win, called the same condition being trapped outside the other man's decision cycle, and it is a losing place from which no amount of diligence will rescue you.[15]

[15] **Two frames.** The strategic vocabulary here is John Boyd's, the OODA loop and the contest of decision cycles, from his unpublished briefings "Patterns of Conflict." The moral frame is Norbert Wiener's, from *The Human Use of Human Beings* (1950), the book that worried, before anyone else, about men reduced to components of a machine that uses them.

There is exactly one way out of that trap, and it is to stop orienting on what the adversary can change and start orienting on what he cannot. He can mint ten thousand domains and ten thousand subject lines for nothing; but he is still selling the same small handful of lies, because only a few lies actually work on a frightened human being, and a lie, unlike a domain, has a shape.[16] So I stopped matching domains and began matching the con itself: the pitch, the campaign family, the recognizable architecture of the swindle. The ACA come-on that fishes for the newly laid-off; the "guaranteed acceptance"insurance hook; the debt-relief lead generation; the brand impersonation carried down to the expiring loyalty points. When a single operation rotates its wrapper from HealthCareCom to Colonial Penn to National Debt Relief in the course of one afternoon, the domain changes and the sender changes and the artwork changes, but the pitch does not, and the pitch is what I now catch. He can swap his disguise every hour; he cannot change his gait, and one learns, in the end, to read the walk beneath the costume.

Before I let one mailbox stand for the world, I held it against the world, and the two did not agree. I looked at global statistics. My own volume had leapt forty-fold; the world's, over the same months, was falling. Microsoft, which stands athwart some eight billion phishing messages in a quarter and can therefore count what I

[16] **The measurers.** I came to "orient on the invariant"the slow way, from my own headers; the academic measurers got there twenty years ago with instruments I will never have. Chris Kanich and colleagues ("Spamalytics,"2008) infiltrated a working botnet and put the conversion rate of spam at about one sale in twelve million messages, which is why so few lures can pay; Kirill Levchenko and colleagues ("Click Trajectories,"2011) traced nearly a billion spam URLs and found ninety-five percent of the goods monetized through a handful of banks, a narrow waist a defender could strike, and the one the modern lead-generation economy has since dispersed. The honest caveat: both studied the pharmacy-and-replica trade of their day, not the lead-generation mail that fills my box. The structure carries over; the particular bottleneck does not.

cannot, reports the raw tonnage in gentle decline through the spring of 2026 even as the craft inside each message sharpens.[17] The honest reading is not the flattering one. What came for me was not the leading edge of a global tide; it was aimed, a campaign that found my address and added it to its targets, while the wider weather, if anything, eased. The disagreement, here as with the clock and the headers, is the finding. What is closing does not announce itself as a louder flood; it comes quieter, and better aimed, and harder to see. The world is not sending more spam. It is sending spam that has learned to write. I was merely awakened from dogmatic slumbers.

Does anyone go to prison for this? The answer is a lesson in how enforcement lags architecture. They used to go to prison, regularly and famously, in the age of the great spam kings. Robert Soloway, who styled himself the Spam King, was indicted in Seattle and sent away for years; Alan Ralsky and his confederates pleaded guilty to a stock pump-and-dump run entirely by email; Oleg Nikolaenko was arrested as the operator of "Mega-D,"a botnet credited at its peak with a third of all the spam on Earth; Jeanson Ancheta drew federal time for renting out a botnet; Peter Levashov of the Kelihos network was taken in Spain and pleaded guilty in an American court.[18] Ev-

[17] **The larger weather.** Microsoft Threat Intelligence reported roughly 8.3 billion email-based phishing threats in the first quarter of 2026, the monthly volume declining from 2.9 to 2.6 billion across January through March even as the delivery techniques grew more elaborate. The honest caveat: Microsoft's vantage is the enterprise inbox and credential phishing, not the consumer lead-generation mail that fills mine, so I cite the global trend as a structural mirror, not as a measurement of my own flood. See microsoft.com/security/blog, "Email threat landscape: Q1 2026."

[18] **The spam kings.** Robert Soloway was indicted in Seattle in 2007 and imprisoned; Alan Ralsky and confederates pleaded guilty to an email-driven stock pump-and-dump; Oleg Nikolaenko was arrested in 2010 as operator of the "Mega-D" botnet, credited with roughly a third of the world's spam; Jeanson Ancheta drew prison for a botnet-for-hire; Peter Levashov of the Kelihos botnet was taken in Spain and pleaded guilty in the United States. See spamhaus.org's ROKSO file

ery one of those cases shares a shape, and the shape is the point: a single identifiable kingpin, a consolidated and profitable operation, a durable business or botnet holding assets a court could seize, and a defendant who lived somewhere a subpoena could reach.

That shape is precisely what the modern operation has engineered out of existence. There is no kingpin, only an operator renting other people's machines. There is nothing to seize, because the domains are worth a dollar and already dead and the servers belong to someone else. There is no one to subpoena, because the operator sits in a jurisdiction that will not answer the telephone. And the lead-generation economy that ultimately pays for all of it is so thoroughly laundered through layers of advertisers and brokers and "publishers"that no single party can be said to hold the bag; the insurance lure and the membership lure, followed home, deliver the curious not to a pharmacy but to a political action committee and a lead-capture form.[19] The takedowns that do reach the news now are for malware, ransomware, and denial-of-service, not for commercial mail: DanaBot, Qakbot, RapperBot, the rest.[20] The men who went to prison were caught because they had built empires; the operation in my inbox was built, with some care, to be no one's empire at all.

---

on Soloway and the Wikipedia "List of spammers."

[19] **Following the links.** Read past the lures to where the links point and the money begins to show its shape: the insurance and "membership"come-ons funnel to political action committees and lead-generation fronts (stoprepublicans.com, turnoutpac.org, boldpac.com), the tool and gift lures to disposable lead-capture redirectors (quotecapture.com, sellingclick.com). The lure's topic and its destination diverge by design; that gap is where the laundering happens. The reading stops at the first redirect, which is as far as one can go without fetching pages one would be a fool to fetch.

[20] **What gets prosecuted now.** The headline takedowns of 2025 and 2026 are malware and denial-of-service operations rather than commercial mailers: the DanaBot indictment of sixteen defendants (May 2025), the Qakbot leader's indictment (June 2025), and the RapperBot and KimWolf botnet cases. See justice.gov's Qakbot release and securityweek.com on RapperBot.

Step back from the spammers, who are only the symptom, and the disease comes into view, and it is structural rather than criminal. Email's entire trust model rested on a quiet wager that sending carried a cost, that a credible sender had something to lose. Artificial intelligence has now driven the cost of a credible, fraudulent sender down to roughly a dollar and a few seconds of generation; and once the cost of forging a sender falls below the cost of verifying one, the open commons is doomed not by malice but by arithmetic. The noise rises faster than any open protocol can price it in. This is the climate change behind my private cliff, and it is why the great walled gardens win.

It is worth being precise about why they win, because the reason is not the one their marketing implies. Gmail's advantage over a man like me is not that it is cleverer; it is that it has more sensory tissue. It stands athwart the path of a billion messages, sees a new campaign's first hundred within seconds, and inoculates the other billion mailboxes before lunch; I meet each campaign cold, one envelope at a time, and learn its shape only after it has already reached me. That is the entire moat. And it is why a commons of this kind dies not in fire but in enclosure. The independent operator is not burned out overnight; he is taxed, slowly, into eccentricity, until running one's own mail is an antiquarian's hobby, and everyone else has filed, gratefully, behind the walls, where their correspondence is read, scored, and sold back to them as the rent. This latter is why I still run my own domain, and my own mailserver.

The collapse in the cost of generation that armed the spammer has also armed his opponent; the mirror of cheap generation is cheap discrimination, and the very class of model that can write a convincing swindle can, on a machine I own and at no marginal cost, read one and recognize its gait. I am no longer outgunned on judgment. I run that tooling actively, managed, in a fast loop, and it mostly

works. I am outgunned on one axis only, and it is the one a lone operator cannot manufacture: reach, the breadth to have been the first to see a campaign. That is Gmail's whole moat, and no amount of local cleverness closes it. The cooperatives one might dream up to pool that reach were tried, anonymously and at the scale of the open internet, in Vipul's Razor and the Distributed Checksum Clearinghouses, and were poisoned and gamed into uselessness;[21] they hold, if at all, only inside a Dunbar's-number cohort of people who already trust one another, and a commons that small dies of the lone maintainer's exhaustion long before it dies of any attack. Scale is hard.

I will not dress any of this as victory. Every defense available to me guards the inbox; not one of them touches the outbound road. When I send a letter outward it is still Gmail and Outlook who decide whether it reaches their billion users or drops, silent and unseen, into a folder I will never be shown, and they make that ruling on a reputation a small and honest sender cannot accumulate by any means available to him. The keep is defensible; the roads belong to the gardens. And there is a quieter danger past the road. The friendly counterfeit the spammer buries in his markup does not die in my Spam folder; scraped up to train the next machine, it teaches that machine what a human is supposed to sound like. Dormant is not dead.[22]

[21] **Razor and DCC.** Vipul's Razor and the Distributed Checksum Clearinghouses were collaborative spam filters that pooled fuzzy fingerprints of messages across many independent sites. Run anonymously and at the scale of the open internet, both suffered poisoning and gaming; that failure is exactly the one a small, mutually acquainted cooperative is positioned to avoid, which is the whole argument for staying small. It is also exactly the filter the leaked prompt's per-recipient token is built to defeat.

[22] **Dormant is not dead.** The phrase, and the discipline behind it, are from a companion essay, "Animism, Theory of Mind, and Participation" (https://www.tauzero.com/Rob_Tow/essays/animism.html): stored organiza-

So the aim was never to defeat the giants. A man whose correspondence is read, scored, and sold has been demoted from a correspondent into a data-point, put to the machine's use rather than his own, which is the reduction Norbert Wiener spent his last clear years warning against, the human being made a component of a machine that uses him. Guy Debord had a blunter name for the same condition, The Spectacle, in which life is no longer lived but watched, scored, and sold back to the one who used to live it. I keep my own mail, on my own iron, read by no one's marketing department or AI scrape, for the reason a man keeps a garden or a workbench: not because it will bring the giants down, but because it is the one channel where I am still a correspondent and not a data-point. And still, at the gate of even that channel, the old sentry's challenge goes up into a dark it can no longer see across: *who goes there?* I can no longer be certain of the answer. The Thing has learned to give it in a friend's voice.

Originally published on tauzero.com and Substack, June 2026.

tion is not inert, only waiting for the loop that lets it act again. A paragraph of counterfeit correspondence, harvested into a training corpus, is exactly such a latency.