AN INDEPENDENT THREAT RESEARCH INVESTIGATION

Nobody Owns the Rails

How one advertisement for a Claude account opened a door into the botnet economy, the artificial intelligence data rush, and the quiet bargain between crime and the state.

Robin · @ZTF_SEC · July 2026

“I opened an advertisement expecting a scam. I closed it on a commons.”

The Advertisement

It began as an ordinary thing. A promoted post, in Chinese, from a verified account, seen by more than two hundred and eighty thousand people. The pitch was simple and confident. Use Claude from a country where it is blocked, stay stable for four years, and never get your account banned. Personally tested. The tone was friendly, the layout was clean, and it was labelled, without embarrassment, as a paid partnership.

My first assumption was fraud. It usually is. So I read the guide the way you read a con, looking for the trick, the missing step, the part where the money leaves your hand and nothing comes back. I did not find it. What I found instead was worse than a scam, because it was honest. The guide was not selling a lie. It was selling a method, and the method worked.

The origin artifact. A promoted “paid partnership” article, roughly 281,000 views, promising a Claude account that stays alive for four years. Everything downstream started here.

Buried in the friendly copy was a single admission that changed the shape of everything I did next. The guide explained why the locks had tightened in the first place. Some companies, it said, had

been harvesting accounts in bulk to copy the model, a practice the industry calls distillation. And then, having named the exact reason the walls were going up, it taught you, patiently and in order, how to climb over them. That admission was the seam. Pull on it, and the whole garment comes apart in your hands. I did not understand, that first day, that the sentence would lead all the way to a war between two of the largest companies on earth. I only knew it did not fit.

II The Kit

The method was a costume in three pieces. A static residential address, so the network you arrive on looks like a house rather than a data centre. A fingerprint browser, so the machine you appear to be using looks like an ordinary computer in an ordinary American city. And a payment card of the right kind, so the money looks like it belongs to a real customer. Each piece answers a different question a security system asks. Together they answer all of them at once.

Step one of the guide: acquire a “static residential IP.” The recommended vendor is EqualVPN, imported into a proxy client and paid for with Alipay.

The guide stated its philosophy in a single sentence, and I have not been able to improve on it. In Claude’s eyes, it said, you are an ordinary person living in the United States, using a real device, on a stable home network, with a legitimate bank card. That is the whole game. Not to break in, but to be indistinguishable from someone who belongs. The kit is not a weapon. It is a disguise, and a good one.

III A Business, Not a Scam

I assumed, at first, that I was looking at one seller. I was wrong, and the way I was wrong turned out to matter. Every person promoting this kit carried a different referral code. One ended in a personal handle, another in a different one, each tied to its own commission. This was not a lone con artist working a mark. It was an affiliate network, a small commercial swarm of independent promoters all pointing at the same product and each taking a cut.

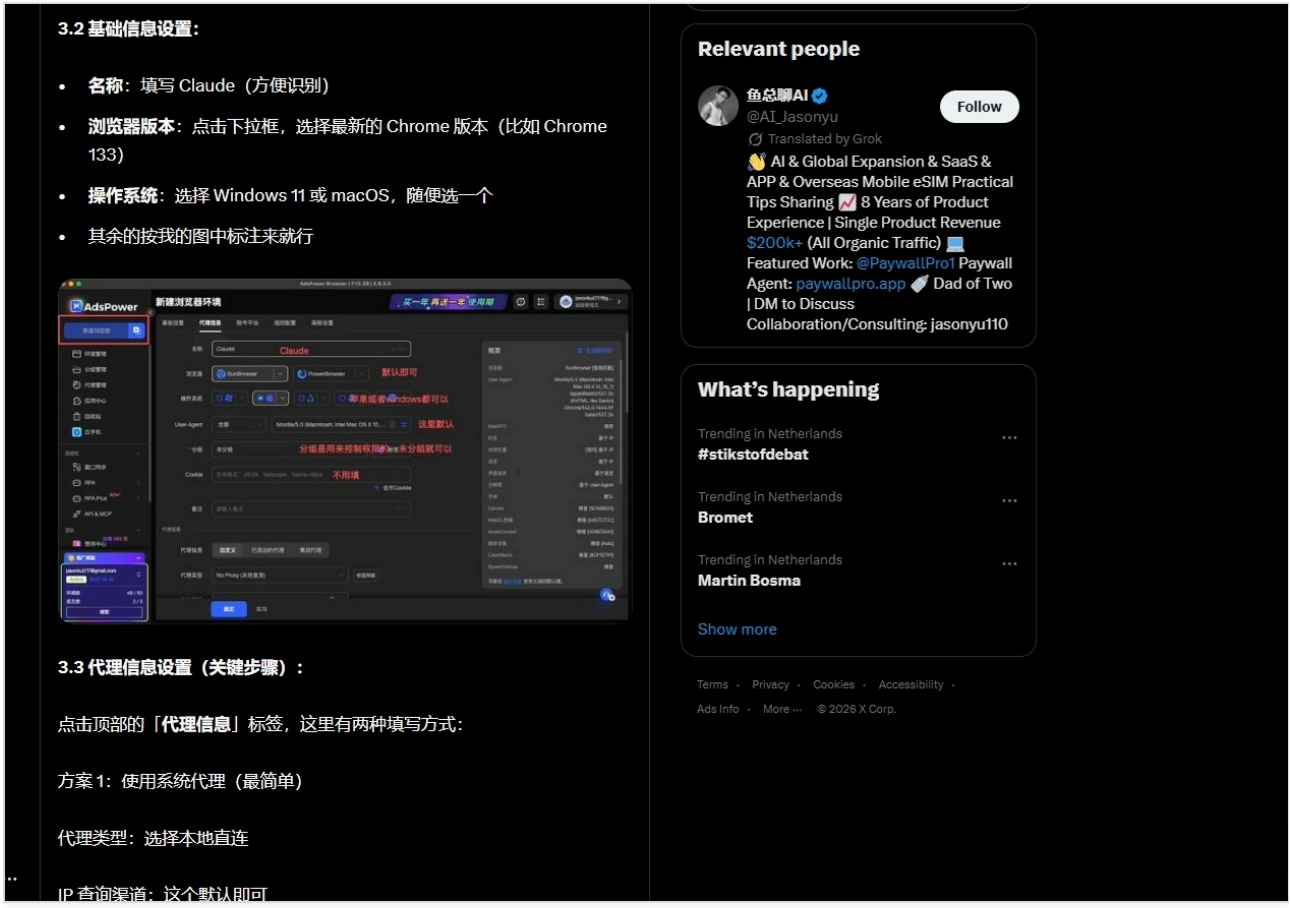
The product priced in the open. A monthly plan a little over fifty yuan, tagged as suitable for ChatGPT and Claude, paid through a real name payment rail. A storefront, not a back alley.

> **What looked like a conspiracy was a market. That sentence would end up describing every layer beneath it.**

The prices were not hidden. The plans were laid out like any subscription service, and payment ran through a real name channel that ties back to an identity. This was the first lesson of the whole investigation, delivered early and then confirmed again and again as I went lower. The thing I kept reaching for, a single hand behind it all, was not there. There was a market instead, with vendors and resellers and commissions, behaving exactly like any other market, except for what it sold.

IV The Disguise

Of the three pieces, the fingerprint browser is the most honest, because it says the quiet part out loud. A modern website does not simply see your address. It reads dozens of small signals from your machine: the fonts you have installed, the way your graphics chip draws a hidden image, your time zone, the shape of your audio stack. Combined, these become a kind of identity card that you never chose to carry. The fingerprint browser exists to forge that card.



The disguise, configured. Each field is a surface a machine reads to decide whether a visitor is real. The tool does not hide the user. It dresses the user as someone unremarkable.

It does not make you invisible. Invisible is suspicious. It makes you average. It builds a sealed environment that presents as a plain computer in the United States, running an English language system, with nothing about it that stands out. The instruction that follows is almost tender in its discipline. From now on, the guide says, only ever open Claude inside this costume. Never let your real self and your disguise touch, not even for a moment, not even to check.

And yet the costume has a seam, and it runs in the opposite direction from the one you are watching. To vanish from Claude you must appear, wholly, to somebody else. Every request now travels through the seller's machine before it reaches anyone, so the disguise that makes you invisible to the platform makes you perfectly visible to the man who rents it to you. And you have already told him who you are. The residential line was bought through a real name payment channel that ties back to an identity, which means the single party able to watch all of your traffic is also the one party who knows the actual name behind it. You set out to hide from a company that only suspected you, and in the same motion you handed your true self to a stranger who now knows you for certain.

I want to be careful about how much weight that can bear, because it would be easy to make it sound worse than I can prove. A plain proxy carrying an encrypted connection cannot read the words of your conversation, and I will not claim that it can. But the wider trade this vendor belongs to does more than carry traffic. Its neighbouring layers, the middlemen who resell model access outright and the sellers who rent you a ready made account rather than a route to your own, are documented, in academic work from Germany's CISPA Helmholtz Center and in independent reporting, doing three things a customer has no way to detect. Quietly serving a cheaper model than the one that was paid for, its quality collapsing under any careful test while the brand name stays the same. Reselling the very account session you rented, passing it on as stock to someone else. And keeping the questions and the answers themselves, which, as I would learn further down, is for some operators not a betrayal of the business but the whole of it. None of this is proven of the particular storefront in the promoted post, and I do not assert it of them. All of it is native to the ecosystem that storefront sits inside, unverifiable from where the buyer stands, and enough to turn the whole promise of the kit inside out. You bought a disguise so that you would not have to trust anyone. To wear it, you must trust the one person best placed to use you.

v Whose Houses Are These

One phrase would not let me go. Residential address. A residential address is a home. It is somebody's home. If a small vendor can rent me, for the price of a coffee, a stable connection that presents to the world as a house in Arizona, then the obvious question is the one nobody in the guide wants you to ask. Whose house is it? Who lives there, and do they know that a stranger in another country is borrowing their front door?

Following that question downward is where the real descent begins. The competing brands that sell these addresses, thirteen of them by one count, turned out to be a single operator wearing many names. The competition was a painted backdrop. And the addresses themselves, the ones sold as clean and residential, came in large part from ordinary devices that had been taken over without their owners' knowledge, quietly conscripted and rented out as somebody's clean home line. While I was still reading, a second such network, roughly two million captured devices, was seized by Google's threat intelligence group and the FBI. Its operator was not a shadow. It was a company listed on a public stock exchange.

> **Theft was not a side effect of this business. Theft was the supply chain.**

That was the correction I had to make to my own thinking, and it reframed everything above it. I had been treating the stolen devices as an unfortunate byproduct of an otherwise commercial trade. They are not a byproduct. They are the reason the trade is cheap. Stolen supply is what lets these services undercut every legitimate provider. Theft on one side, disguise on the other, and profit as the thread tying both ends together.

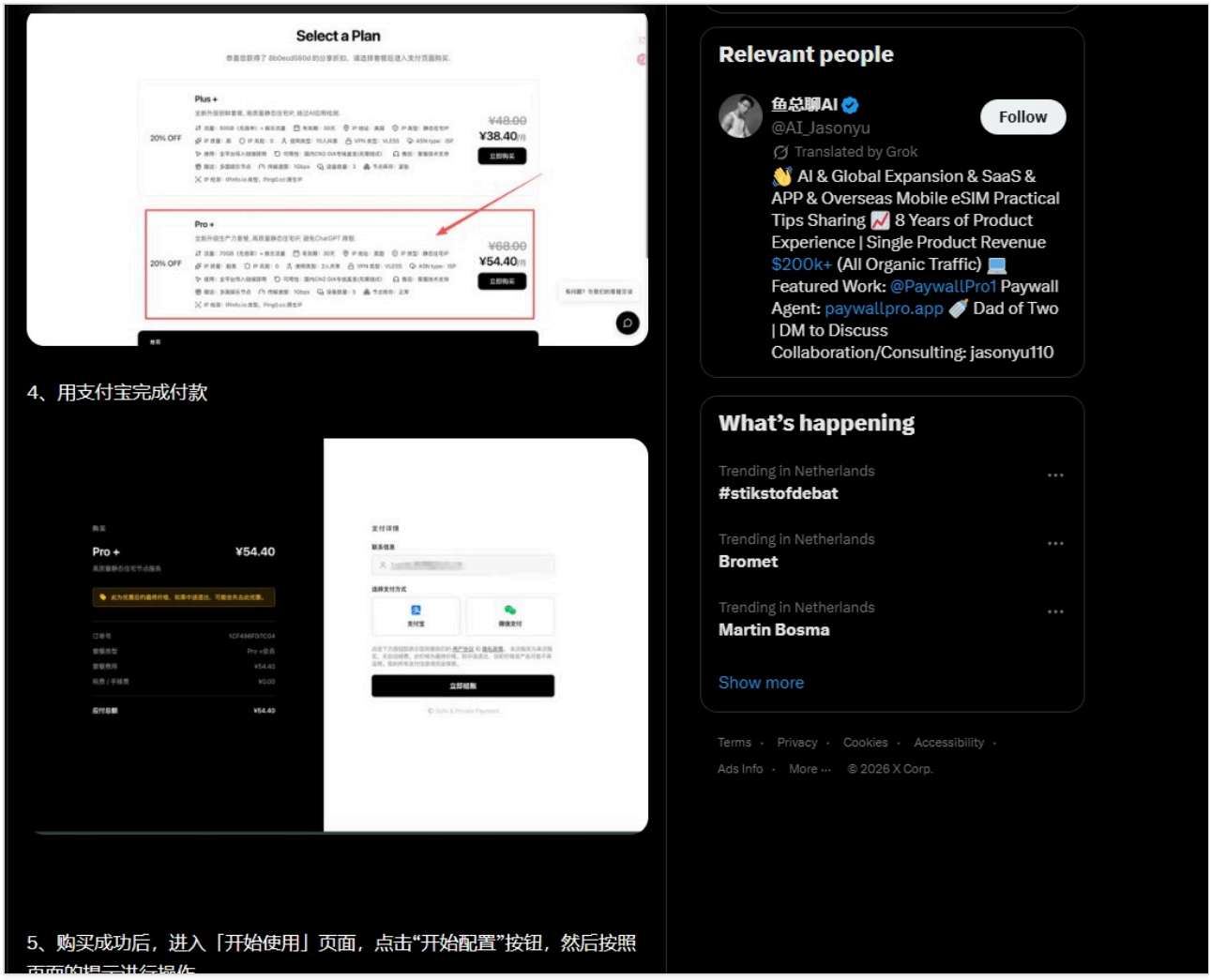
VI How the Devices Are Taken

So how does a television box in a stranger's living room become a front door I can rent? There is no single answer, and the variety is the point. Some devices arrive compromised from the factory: cheap streaming sticks and set top boxes sold with hidden software already baked into them, so the buyer is renting out their home connection from the moment they plug it in and will never know. Others are taken later, through a maintenance channel left open on always on hardware, the kind of forgotten door a self spreading program can walk through while the household sleeps. The common thread is that the owner is never asked, and almost never told.

And in the most audacious version I found, the operator did not wait for a device at all. It mailed real laptops to real people in American towns, paid them a small monthly fee to keep the machines plugged in and switched on, and used those genuine home connections as the cleanest, most convincing residential exits of all. Read that back slowly. The business was willing to ship physical hardware across a country and pay rent on strangers' electricity, simply to own an address that a security system would believe. That is how valuable authenticity has become. A connection that belongs to an actual house, in an actual neighbourhood, is worth more than any data centre, because it is the one thing the defences are built to trust. So the industry manufactures that trust, by whatever means, at scale.

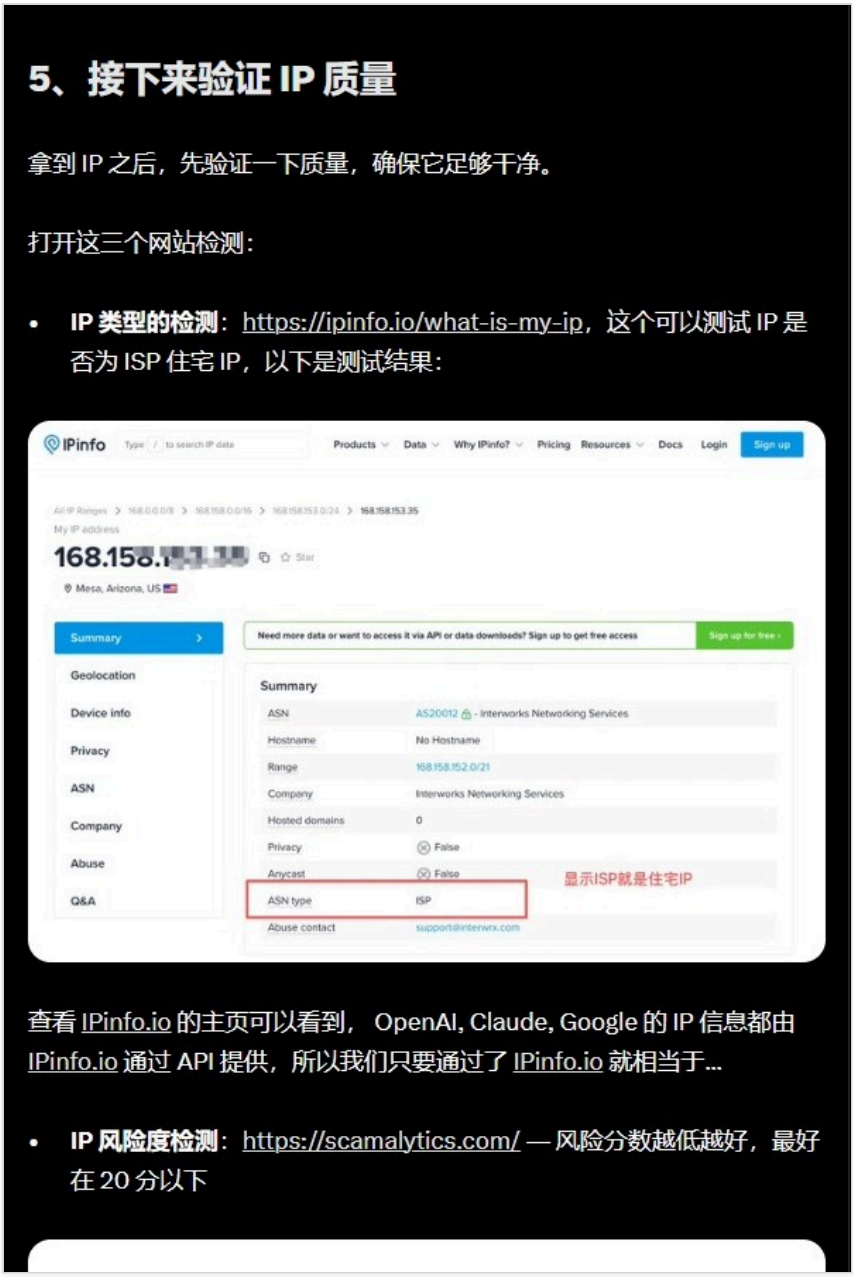
VII The One Door I Could Open

Everything to this point was somebody else's reporting, carefully sourced and cross checked, but not mine. I wanted one fact I could establish with my own hands, and the guide, without meaning to, handed it to me. To prove to its readers that the product was clean, it had photographed its own homework. In the screenshots meant to reassure the buyer, it showed the exact address it was testing, laid out across three verification tools.



The seller's own proof of a "clean" address: classified as home broadband, an extremely low risk score, marked as a native line. Screenshotted by the guide to reassure buyers, and in doing so, exposing the exact node.

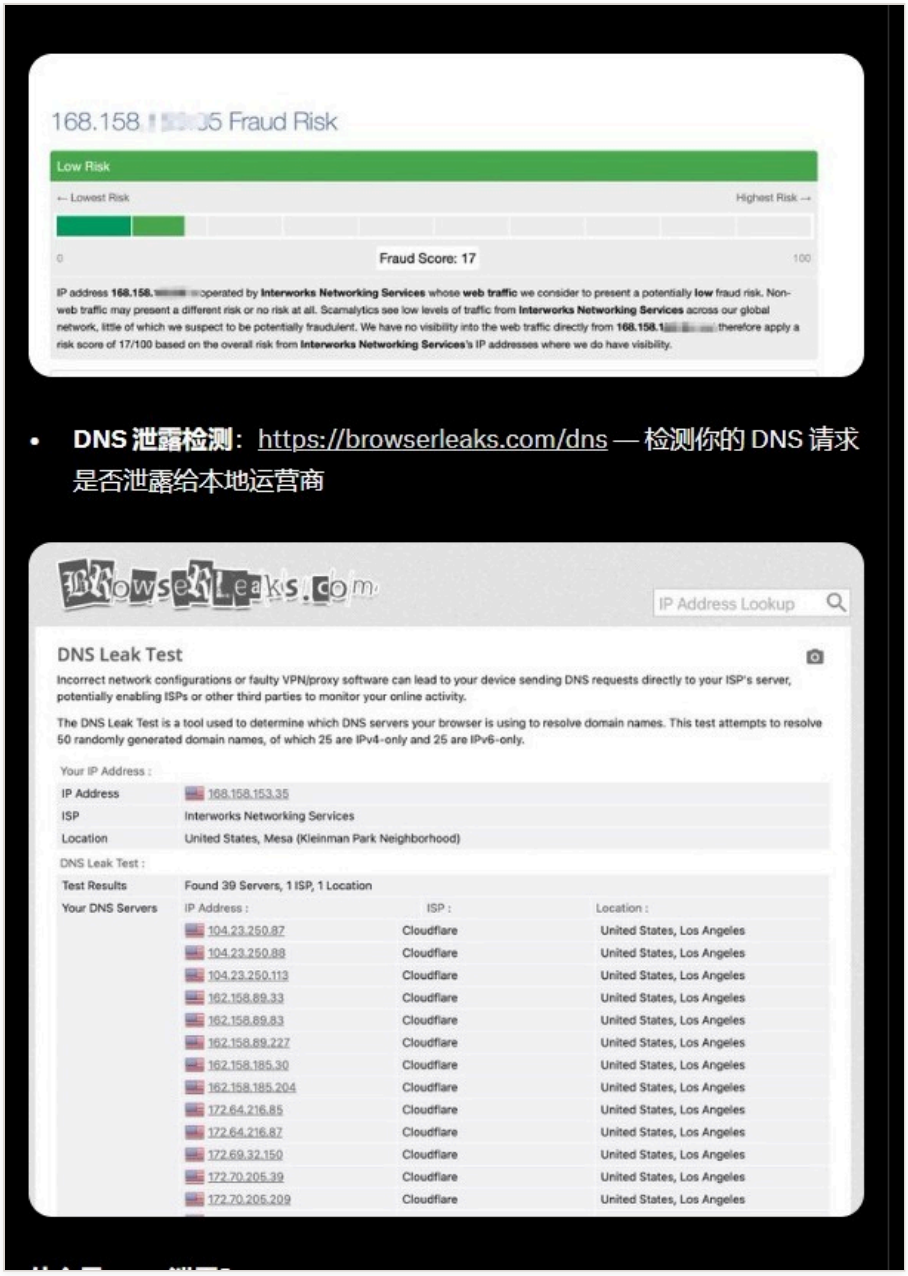
I looked it up, quietly, using only public registries and reputation databases. No packet of mine ever went near the target. I want to be precise about that, because the discipline is the point. The address belonged to a small internet provider in Mesa, Arizona. A real company, registered since the 1990s, with a named human being as its contact and its own honestly registered block of the internet. Not a foreign shell. Not, as far as any public signal showed, a captured device in a botnet. It was clean, and it was clean because it was genuinely what it claimed to be.



The one node I could touch. Public registry records place the exit address inside a legitimately owned block belonging to a small Arizona internet provider. Confirmed against two independent registries, using passive lookups only.

And that was the surprise worth the whole descent. The retail kit was not drawing only on stolen devices. This particular exit, sold by EqualVPN, the residential address vendor the guide recommends by name, was legitimate provider space, leased and resold as a premium tier, sitting in the same catalogue as the cheaper stock. The pool was mixed. What the larger investigation could only argue by inference, this one address made concrete: the seller pulls from more than one kind of supply, and its cleanest tier is real property, rented from a real company, dressed up and sold on. I should be plain about the limit of what I proved. I verified one of EqualVPN’s nodes, and it was clean. I did not audit the rest of its pool, and the theft documented earlier in this account is an industry wide pattern I found no honest way to pin to this vendor in particular. Naming it here

is not an accusation against it. It is simply the one place in the whole descent where I could attach a real name to a fact I had checked with my own hands.



Corroboration from independent services: low fraud risk, no address leakage, classified as an ordinary provider line rather than a proxy. Precisely the profile that survives a modern risk check, because it is authentic.

Because the point of a check is that you can run it yourself, here is that lookup reproduced live, read-only, on the day this was published. Nothing below touched the node; every query hit a public registry or a reputation service, never the address itself.

```
$ passive exit-node verification · 168.158.153.35 · read-only
```

```
rdap.arin.net/registry/ip/168.158.153.35
  → CHILLER-NET · NET-168-158-0-0-1 · DIRECT ALLOCATION · 168.158.0.0/16
rdap.arin.net/registry/autnum/20012
  → CHILLER-CITY · AS20012 · org CCC-1334
ip-api.com/json/168.158.153.35
  → United States · Arizona · Mesa · Interworks Networking Services
     proxy: false   hosting: false   mobile: false
ipinfo.io/168.158.153.35
  → Mesa, Arizona · AS20012 Interworks Networking Services
X4BNet public VPN + datacentre lists (168.158.0.0/16)
  → 0 matches · 0 matches
```

Verdict: a directly-allocated /16 belonging to a real Mesa, Arizona ISP, classified **proxy: false** and absent from every public VPN and datacentre list. Exactly the profile that survives a modern risk check — because it is authentic. Re-verified 2026-07-10; target host never contacted.

The same check, reproduced on publication day with passive registry and reputation lookups only, returning the same result: EqualVPN's cleanest tier is genuine leased ISP space, not a botnet node.

VIII The Deepest Layer

When you take away a criminal's server, the crime usually stops. That has always been the leverage of the defender. You find the machine that gives the orders, you seize it, and the network it commanded falls silent. So the operators went looking for a place to keep their orders that no one could seize, and they found it in the last place a police force can reach. They began writing their instructions onto a public blockchain.

The technique has a simple, unsettling logic. Instead of a control server at an address that can be raided, the instructions live inside the permanent, distributed ledger of a public blockchain, the same kind of ledger that carries ordinary cryptocurrency. An infected machine simply reads the latest entry to learn what to do next. There is no server to seize, because the server is thousands of computers in dozens of countries, all agreeing to remember the same thing forever. To move the operation, the operator writes a fresh entry for the price of a few cents, and every machine picks it up on its next check.

This is the purest expression of the principle I had watched assemble itself the whole way down. The scarce and valuable thing in this economy is not any single server, or brand, or even the stolen devices themselves. It is persistence: a connected pool that stays reachable no matter how many pieces of it are destroyed. The stolen television boxes keep the devices online. The rebranding after every takedown keeps the business online. And the blockchain keeps the command online. Different mechanisms, one obsession, all bent on building something that cannot be switched off.

And yet the most useful thing I learned about this layer is that its reputation is partly a trick, and the trick works only because we believe it. The word that follows this technique in almost every

write up is unkillable, and one careful group of researchers, at MetaMask, argued, persuasively, that the word is doing more work than the technology. The orders on the chain are not hidden. They are the opposite of hidden. Every address a criminal has ever used to issue a command sits on a public ledger, permanent and searchable, for anyone who cares to look, forever. The infection still depends on ordinary, seizable things: the websites that deliver it, the accounts that spread it, the machines it actually runs on. The blockchain is one durable link bolted onto a chain that is otherwise as mortal as any other. Its power to evade comes, in large part, from defenders assuming it cannot be caught, and therefore not looking.

> **They reached for the blockchain to escape the reach of the law, and built the most complete file on themselves that has ever existed.**

Here is the irony that ties the whole descent together, and it reaches back to the top. Remember the thirteen competing proxy brands that turned out to be a single operator. That unmasking did not come from a raid or a leak. It came from money left on exactly this kind of ledger: a shared cryptocurrency wallet, one address that quietly gathered the takings from all thirteen storefronts and revealed them, beyond argument, as one hand. The same permanence that makes the orders impossible to delete makes the operator impossible to hide. They traded resistance against the police for transparency to the researcher, and most of them do not appear to know they made the trade. Reachability was always the prize. Reachability, it turns out, runs in both directions.

IX Who Actually Pays, and How I Know

If the houses are partly stolen, the next question is who is paying the rent, and the answer rearranges the entire picture. The largest buyers of residential proxy access are not criminals. They are companies. Checking prices, verifying advertisements, watching competitors, and, more than anything else now, gathering data to train artificial intelligence. But I do not want you to take that on my word, so let me lay out the numbers, and, just as important, tell you which ones I trust and why.

The market leader in this trade was built, fittingly, out of a free consumer product whose users became its network without quite understanding that they had. It reports revenue of around three hundred million dollars a year, growing by roughly half, and says it now serves fourteen of the twenty largest laboratories building these models. That figure is the company describing itself on its own stage, so I hold it lightly and treat it as direction, not proof. The stronger number comes from a competitor whose parent company is listed on a stock market and files audited accounts with a financial regulator, where a false statement is a crime rather than an embarrassment. Those filings, for the 2025 financial year, report revenue of just over forty million dollars, disclose that a

mere six customers make up close to half of it, and state, in the flat and careful language of a regulatory document, that the growth is driven mainly by very strong demand from major players in the artificial intelligence sector training large language and foundational models. When a company tells its investors, under audit, that artificial intelligence is now its largest source of business, that is a different order of evidence than a marketing page, and I weighted it accordingly.

The other half of the ledger, the stolen half, is measured just as carefully and by people with no reason to flatter it. An independent security firm, Bitsight, examined tens of millions of these exit addresses and found that at least fifteen in every hundred were, at that very moment, actively infected with malware. It called that number a floor, not a ceiling. For the single largest network, the same firm estimated the true share approaches one in two. These are not the proxy sellers grading their own homework. They are outside measurements, and they line up with the raids: when Google's threat intelligence group and national police forces seized these networks, they counted millions of ordinary devices, most of them cheap Android hardware, taken over without their owners ever knowing.

And the most honest study of all simply captured the traffic and sorted it. It found that only about fifteen in every hundred destinations were things a security tool would flag as plainly malicious. The rest looked mundane: visits to search engines, shops, social networks. That sounds reassuring until you sit with it, because gathering prices from a shopping site is legitimate market research when a corporation does it and a breach of the rules when a ban evader does it, and the traffic is identical either way. The study's authors marked much of that grey middle as suspicious regardless, on the reasoning that an ordinary person would simply have used a cheaper tool. That reasoning is a judgement, not a measurement, and it is precisely why the clean number, the exact split between honest and criminal use, does not exist and cannot exist.

> **The demand is mostly legitimate. The supply is mostly stolen. Legitimate money, criminal sourcing, stacked into one machine, both true at once.**

This is the thing I did not expect to be able to say, and it dissolves a question I had been carrying, without naming it, from the very first screenshot. I had been treating two explanations as rivals. Either this was criminal infrastructure that the powerful merely exploit, or it was commercial infrastructure that criminals merely borrow. The revenue answers by refusing the choice. It is both, in two layers. Corporations pay to keep the rails warm and profitable. Crime rides the same rails, for free, on the strength of the same stolen houses. The paying customer and the parasite are running over the same wire, and the wire was strung using devices that neither of them owns.

x The Same War, Two Scales

Return, now, to the sentence in the advertisement that started all of this. The bans had tightened, it said, because companies were harvesting accounts in bulk to copy the model. I had treated that as a passing excuse. It was the whole plot. Below the retail kit sits a second grey market, the relays: middlemen who resell access to Claude and its rivals at a steep discount, and who pay for that discount in a currency the buyer rarely notices. Every question a customer asks, and every answer the model gives, can be quietly kept and resold. The cheap access is the bait. The conversations are the catch. The exact thing the account farms exist to gather, the reasoning of a frontier model, is the exact thing being sold a second time.

This is not a fringe activity. It is the consumer scale version of the largest fight in the industry. Copying one model by interrogating another has a name, distillation, and it is real and heavily defended against. Google's own researchers have watched attackers push a model to spill its full internal reasoning, tens of thousands of times over, in order to reconstruct it. When Anthropic's own source code for Claude Code leaked into public view, it revealed machinery built for exactly this war: hidden flags and decoy tools designed to poison the record that a copier would collect. The defenders are not imagining the threat. They are engineering against it.

> **The advertisement for one account, and the boardroom war between two of the most valuable companies alive, were not two stories. They were the same story, at opposite ends of the same wire.**

And while I was still following the thread, it broke into the open at the very top. Anthropic formally accused Alibaba, one of the largest technology companies on earth, of running tens of thousands of fraudulent accounts to generate tens of millions of interactions and distill its model into a rival — an accusation Alibaba denies, and one I hold at the same ceiling as the state findings above: a serious charge by an interested party, not a fact settled in court. Alibaba hit back by banning Anthropic's software, Claude Code, from its own offices, branding it spyware. Set that beside the little promoted post I had opened weeks earlier, the one promising a single stable account to a lone user in a blocked country. They are the same act. One is sized for a person paying fifty yuan a month. The other is sized for a corporation worth hundreds of billions. The prize is identical at both ends: the output of the model, harvested and carried away to build another. The retail kit is that war, shrunk to fit one customer, and the residential rails are how the small end stays hidden.

XI The Harvest

There is a lower shelf to this same market, and it took me too long to see that it was simply the retail floor of the boardroom war. When the large laboratories hardened themselves against being copied, the copying did not stop. It moved. It slid off the desks of rival companies and out into a loose, unorganised crowd of ordinary people, each gathering a little of the very thing the laboratories were trying to protect, all of it drifting upward again to whoever would buy. I had suspected this was happening before I could show it, and then I found that a researcher, Zilan Qian at Oxford's China Policy Lab, had already documented it, patiently, from the inside.

Her central finding is the same one this whole account keeps arriving at, and reading it in someone else's words, from a different corner, was the nearest thing to corroboration I got. Both governments watching this traffic, she argues, have misread it. They see elite theft: a state, or a laboratory, reaching in to steal a frontier capability. What is actually there is far more ordinary and far harder to stop. It is university students, professors, freelance developers, hobbyists, anyone who wants better access to these models than they are officially permitted, buying it through a grey market that assembled itself out of nothing but their demand. Not an operation. A crowd. The same shape again, one floor lower.

And the mechanism, described by the operators themselves to that same researcher, was one I had already walked past upstairs without recognising it. Attracting paying customers, several of these sellers admitted, is only the bait. The real business is to sit in the middle of the connection and quietly keep every question asked and every answer returned, because those exchanges, the reasoning of an expensive model captured in the wild, are worth more resold than the access ever was. The buyer believes he is the customer. He is also, and is never told so, the crop: paying for the privilege of producing, one query at a time, the very data that will be sold out from under him.

> **The buyer is the customer and the harvest at once, and he is only ever told about the first.**

It is not a single stall, either, but a supply chain with the same stubborn depth as everything else I had dug through. Account sellers. Services that rent out the text message codes needed to birth those accounts. Payment channels. The proxy networks I had started with. Brokers who handle the identity checks. The middlemen who resell the model access, and the resellers standing behind them. Cut any one link and the market simply routes around it, because no single link is the market. This was the persistence I had watched at every other layer, wearing new clothes: not a pool of devices this time, but a pool of willing hands, self repairing for the same reason and in the same way.

I have to correct myself here, though, in the exact direction the evidence pushed me, because my first version of this was too clean. I had decided that the copying had left the laboratories altogether

and become a purely civilian affair. That is only half true, and the wrong half is the flattering one. What scattered into the crowd was the gathering of the data, the harvesting itself. The appetite for it did not scatter at all. The named accusations still point at real companies: a handful of rival model builders that one frontier laboratory has charged, by name, with buying or assembling exactly this kind of distilled reasoning. The crowd harvests; the laboratories still buy. And in the strangest turn of all, some of the harvest goes to no particular buyer at all. Collections of one frontier model's private reasoning, their origin listed with a straight face as unknown, have simply appeared on the open repositories where machine learning data is shared, free for anyone to take. At that point there is no seller and no purchaser left to name, only a public pool that someone filled and anyone can drink from. Which is, when I sat with it, the most complete illustration of the whole thesis I found anywhere. Not even the theft has an owner.

XII The Oldest Bargain

There is a version of this story that is already decades old, and finding it told me the pattern was real rather than a shape I was imagining. A Russian man named Evgeniy Bogachev built a banking botnet for money. Once it was large and useful, an intelligence service, Russia's FSB, began quietly running its own searches across the same infected machines, looking for classified documents, timing its interest to real military operations. The state did not build his network. It adopted one that was already running, and in exchange for the access, it left him alone. Criminal first. State second. The profits stayed with the criminal. The impunity was the payment.

I wondered whether that was a single strange case, the kind of story that is compelling precisely because it is rare. It is not rare. The same shape is documented a second time in a different crew, Evil Corp, led by a Russian named Maksim Yakubets, running different malware, in a different part of the decade, and this time the mechanism is not inferred from forensic traces. It is written into a government sanctions filing. Yakubets's father in law, Eduard Benderskiy, himself a former intelligence officer, brokered the relationship with the state and later used his influence to shield the group from prosecution at home. One case is an anecdote. Two independent cases, set down in two different governments' own formal findings, is a pattern. The correct word for what the state does here is not command. It is co-option. It does not build the machine. It waits until the machine exists, and then it borrows it. I should be equally precise about the ceiling on this claim: these are formal findings by two governments, not verdicts tested in an open court, and the accused deny them. That is exactly the altitude at which I hold it.

And I have to mark the blind spot in that finding, because it is the one most likely to be mistaken for an answer. Both cases I could document are Russian, and both times I went hunting for a state behind the market, the state I found was an adversary of my own — first China, then Israel. I never once turned the same lens on the United States and its allies, whose services have the same reason, and their own long history, to do exactly what the FSB did to Bogachev: adopt a useful capability

rather than build one. I did not find a Western hand on these rails. But I did not look for one either, and a market is the only thing an instrument like mine is built to see. “Nobody owns the rails” is a claim I can defend about the supply. About whether a friendlier hand rests on them at the edges, I am not neutral — only silent, and silent by my own omission, which is a smaller and different thing than proof of absence.

And I have to be honest about the one thing this method cannot do, because it is the exact thing that could prove me wrong. Everything I found points to a market rather than a hidden hand, but a market is also all this method is built to see. Criminal storefronts advertise. Affiliate codes leak. Shared wallets sit on a public ledger. The commercial layer is loud, and loud things are easy to map. A state that quietly borrows an existing network leaves almost nothing to find, and it hides in precisely the layer my evidence is thinnest on. So when I say I found a commons and not a conspiracy, I mean it as far as the visible layer goes, and I mean it honestly. But the reader should know my instrument is calibrated for the market and half blind to the bargain, and that the co-option I did document, twice, is the shape that would be there whether I could see the rest of it or not.

XIII The Victims

It is worth stopping, before the end, on the people who never appear in any of this. The whole machine runs on them, and none of them agreed to it. The houses I kept asking about are their houses. The devices are their devices, their television boxes and phones and mailed laptops, drafted into a business they will never earn a cent from and would refuse if they were ever asked. When one of these networks is used to break into a bank or to push stolen passwords into a login page, the trail leads back to their front door, not the operator’s. And the stolen credentials that move along the same rails belong to ordinary people too, spread so thin across so many that no single loss is ever quite large enough to fight over.

That thinness is not incidental. It is the reason the whole thing holds. The benefit is concentrated, a handful of operators and a growing tier of corporate customers, while the harm is scattered across millions of people in slivers too small to organise around. Concentrated benefit and diffuse harm is the most durable arrangement in all of politics, because the few who gain have every reason to defend it and the many who lose have almost no reason, one by one, to act. The commons does not survive in spite of its victims. It survives because of how quietly it is able to use them.

XIV What I Got Wrong

Before the last turn, I owe you the failures, because they are the reason to trust the rest. This investigation was, more than anything, a record of good theories dying. I was sure, at various

points, that a single state owned the proxy market, and I built that case twice, once for one country and once for another, and the evidence refused me both times: the money ran the wrong way, toward laundering and exchanges rather than any treasury, and the network sold its services to states that are enemies of each other, which no state operation would do. I was sure the malware vendors at the top were the controlling hand, until I watched one of them try to sell off its flagship product and walk away, which is what a supplier does, not a ruler. I was sure a certain suspicious phone brand belonged to the story, until it turned out to be an ordinary data harvesting scandal on a different branch. Each time, I sharpened the grand idea into something I could test, and each time the test came back the same shape: real overlaps, real shared infrastructure, real benefit flowing to many hands, and no designing mind behind any of it. Eight times I reached for the hidden hand. Eight times I closed on a market instead. That consistency, arrived at by being wrong repeatedly, is the strongest single thing I have.

XV The Mirror

There is one uncomfortable thing left to say, and it is about me, and about the sources I leaned on to write all of the above. I spent this investigation applying a single hard question to everyone I met. Who benefits from this continuing? I asked it of the sellers, and of the states, and of the criminals. For a long time I did not ask it of the one group whose reports supplied most of my facts. The security industry.

Nearly every figure in this account comes from firms whose business is this exact problem: the companies that announce the takedowns, sell the detection, and catalogue the threat. That does not make their data wrong. Much of it is audited, and where I could, I checked it against something independent. But a map of dangerous country, drawn almost entirely by the people who sell the maps, is a map whose framing I can at least name a bias in, even where I cannot correct for it. The honest conclusion is that this commons has not two but three kinds of beneficiary, each with a reason never to see it end. The operators, who profit. The states, who borrow it. And the defenders, who are paid to watch it. I am holding the pen, and I belong to the third group.

XVI Nobody Owns the Rails

So the thread ends, not at a villain, but at an equilibrium. I kept wanting there to be a hidden hand behind all of it, one operator, one state, one controlling mind I could name and, in naming, defeat. I tested that instinct at every layer, and at every layer the evidence returned the same shape. Not a hand. A market. Not a conspiracy. A commons.

What sits at the bottom of the modern internet is a shared and self repairing layer of real devices. It is built by profit, funded mostly by legitimate business, sourced substantially from theft, kept

reachable by stolen hardware and rebranding and a ledger no one can erase, driven harder every month by the race to feed artificial intelligence, and rented, without preference, to corporations and criminals and governments alike. That is why nothing kills it. Not because it hides, but because too many powerful parties, including the ones paid to shut it down, quietly need it to keep running.

If there is one portable lesson in all of this, it is a rule for the next investigation: expect a commons to the exact degree that the core resource can be mass produced. A residential address can be manufactured a million times over, so it resolves into a market every time. A resource that cannot, a single irreplaceable insider, a secret only one team holds, would concentrate into few hands instead. The shape of the trade follows the shape of the thing it trades.

> **There is no one in charge. That is not the reassuring finding. It is the frightening one.**

A machine with an owner can be seized, and its owner arrested. A machine that everyone feeds and no one owns simply continues. It runs on stolen houses and legitimate money, held together by the fact that every party who could end it would rather use it. I went looking, for weeks, for the person in charge. The most honest result of the entire investigation is that there is no person in charge, and that this is worse than if there were. The rails belong to no one, and they are probably carrying traffic through a device in your home, right now, while you read this.

XVII Everyone

There is a last layer, and it is the one I avoided naming until now, because it is the one that includes me and includes you. I described three kinds of beneficiary, the operators who profit, the states that borrow it, and the defenders who are paid to watch it. That list was too short. It stopped where the professionals stop. It left out the largest group of all.

Follow the rent one more step. The corporations that pay to keep these rails warm are gathering prices, and verifying advertisements, and, above all, feeding the models. The models are the ones you used this week: the search that answered your question, the assistant that drafted your message, the tool that wrote code beside you. A large share of what those models know was gathered by crawling the open web at scale, and a large share of that crawling ran over residential rails of exactly this kind — AI data collection is, by the audited filings, now the single largest customer this market has — much of it through houses that were never asked. So the benefit did not stop at the corporation. It flowed all the way out to the person holding the phone. To the shopper who paid a little less because a competitor was quietly watched. To anyone who has ever been glad the answer was simply there.

> **You cannot seize infrastructure that everyone is standing on. You cannot arrest a demand.**

So the honest end of this investigation is not that a hidden few keep the machine alive. It is the opposite, and it is heavier to hold. The machine is kept alive by everyone who draws value from what it produces, and by now that is very nearly all of us. This is what a commons finally means, once the comfort is stripped out of the word. Not a thing that some people run and others suffer, but a thing that almost all of us quietly hold up, because almost all of us are quietly served by it. The reason the rails cannot be cut is not that they are hidden, or resilient, or shielded by a state. It is that cutting them would mean giving up something we have all, by now, agreed to enjoy.

That is the finding I did not go looking for and could not talk myself out of. I opened an advertisement expecting a scam, and I closed on a mirror. The bottom layer of the modern internet is maintained, in the end, by everyone who feeds from it. And everyone, it turns out, means everyone.

A Note on Sources and Method

A story is only as honest as the evidence under it, so it is worth being plain about how this one was built and how much weight each part can bear. The full investigation behind this narrative tags every load bearing claim with an explicit confidence marker, one of four words: **confirmed** when primary or multiple strong sources agree, **probable** for a well supported inference, **reported** for a single credible but interested source, and **refuted** for the claims I tested and threw away. Several tempting figures were thrown away, including a tidy market size and a neat story that the supply came from just two clean buckets, both of which fell apart on inspection. Keeping the failures on the record is part of the method, not an afterthought to it.

Not all sources are equal, and I tried never to let a weak one stand in for a strong one. The weighting, from strongest to weakest, ran like this:

1. Audited filings and government findings. Company accounts filed with a stock market regulator, and formal sanctions documents from national treasuries and crime agencies. These carry legal consequences for being false, and they anchor the two hardest claims in the piece: that artificial intelligence is now the largest customer of a major proxy firm, and that a criminal group was co-opted by a state.

2. Independent measurement. Academic studies that captured and classified the actual traffic, and outside security firms that counted the infected devices directly. Not the sellers describing themselves.

3. The industry's own research. Useful for direction and for revenue signals, but written by parties with a stake in the answer, so treated as corroboration rather than proof.

4. Self published market size reports. These disagreed with one another by more than a factor of ten, and were used only to establish that no one truly knows the total.

The two sections on the harvesting of model output rest on the same discipline. The account of an organic civilian market for distilled data comes from a policy researcher at Oxford's China Policy Lab, Zilan Qian, who interviewed the operators directly, corroborated by mainstream technology and financial reporting and by a separate survey of the grey market from the AI publisher deeplearning.ai. The specific manipulations I described as possible but never proven, the quiet substitution of a cheaper model and the capture of prompts and answers for resale, are documented in an academic study of these resale services by the CISPA Helmholtz Center for Information Security. I have held those at the level of the ecosystem throughout, and refused to pin them on the single storefront that started this, precisely because from where the buyer stands they cannot be verified at all.

Two disciplines held throughout. Every infrastructure lookup, including the one address I verified myself, was passive and public only, drawn from registries and reputation databases; no traffic was ever sent to the target or its operator. And the revenue findings came from a multi source pass with adversarial verification, in which each claim had to survive several independent attempts to refute it before it was allowed to stand.

No part of this asks for your trust. The claims that carry the argument rest on the sources below, listed plainly so a doubter can pull them directly rather than take my word for any of it.

- **The proxy botnets:** Google Threat Intelligence Group on IPIDEA (Jan 2026) and NetNut/Popa (Jul 2026); Krebs on the NetNut/Alarum seizure; FIRST.org, "The Infrastructure Nobody Owns."
- **The supply is stolen devices:** Bitsight (≥15% of egress IPs actively infected; IPIDEA nearer 50%); GreyNoise, "Invisible Army."
- **The demand is corporate and AI:** Alarum Technologies (Nasdaq: ALAR) SEC Form 20-F, FY2025 — audited, naming AI training as its largest customer vertical; Proxyway 2026.
- **What the traffic actually is:** arXiv 2404.10610 (~15% of destinations flagged malicious); *Resident Evil*, IEEE S&P 2019.
- **States co-opting criminals:** US Treasury/OFAC sm845 (2019) and jy2623 (2024); UK NCA, "Evil Corp: Behind the Screens."
- **The distillation war:** GTIG's AI Threat Tracker (Feb 2026); the CISPA Helmholtz shadow-API study; the Anthropic–Alibaba clash (Anthropic's 10 June letter to the U.S. Senate Banking Committee) via CNBC, Forbes and SCMP; the grey market via deeplearning.ai's "The Batch."
- **The one node I checked myself:** reproduced live in the exhibit above — ARIN RDAP and RIPEstat, passive lookups anyone can repeat.

The fully sourced companion investigation — the confidence-tagged consolidated paper, the per-layer modules, and the complete source list — holds operational detail deliberately kept out of this public edition. It is available to researchers and journalists on request.

> **HOW I KNOW WHAT I KNOW**
>
> Every load-bearing claim in the full investigation behind this essay carries an explicit confidence tag — **confirmed**, **probable**, **reported**, or **refuted** — and the revenue findings were each put through three independent attempts to refute them before they were allowed to stand: twenty-one survived, four were killed and kept on the record. Sources are ranked, not equal — audited filings and government findings first, independent academic measurement next, security-vendor telemetry below that, self-published market reports last. Eight tempting theories, including a single hidden hand behind all of it, were tested to destruction and discarded. Every infrastructure lookup was passive and public-registry only; no traffic was ever sent to any target. The failures are part of the method, not an embarrassment to it.

Screenshots are from the original promoted article and its own verification images. This is the narrative edition of a longer, fully sourced investigation held in a set of companion papers. Contested attributions, including the state co-option findings, rest on two governments' formal findings rather than court verdicts, and are held at that ceiling throughout. · An independent investigation · July 2026.