flare

The Phishing Kits Economy in Cybercrime Markets

By Assaf Morag, Cybersecurity Researcher

In the early days of phishing, attackers didn't need much more than a crude HTML form. The designs were sloppy, the logos were wrong, and sometimes the page didn't even resemble the real service, yet people still typed in their usernames and passwords.

Phishing was fundamentally simple: trick a user into handing over static credentials, and the job was done. Then everything evolved. As organizations adopted stronger authentication, threat actors adapted even faster. Phishing kits became modular, automated, and commercially distributed. Visual templates reached near-pixel perfection.

Today, the landscape is dominated by highly sophisticated phishing-as-a-service (PhaaS) platforms and reverse-proxy kits like EvilProxy, Typhoon, Tycoon 2FA, and others. These systems don't just capture passwords, they can:

- intercept live session cookies
- bypass OTP-based 2FA
- defeat modern MFA flows
- capture dozens of elements in the users' DOM

Phishing has transformed from basic social engineering into a full-scale technical operation, where threat actors leverage real-time man-in-the-middle infrastructure to silently take over accounts with almost no user suspicion.

In this report, we dive into the underground economy of phishing kits through 8,627 instant messaging, open source, deep, and dark web chats to take a closer look at their technical design, including how live phishing servers function in real attacks.

Key Takeaways of Phishing Kits from 8,600+ Chats

- Phishing is now a service economy, not a technique. The dominant products aren't "fake login pages" - they're adversary-in-the-middle (AiTM) / reverse-proxy platforms (EvilProxy, Tycoon2FA, Typhoon, etc.) built to steal sessions, bypass OTP-based MFA, and automate takeovers at scale.
- This research is based on a sample of 8,627 instant messaging, open source, deep, and dark web items from the past year. We used the search terms such as "phishing kits" and "real-time phishing," and removed any duplicates and irrelevant messages. Of those, 3,130 (36.3%) were classified as real threats (high confidence), plus 1,769 (20.5%) suspected-real threats (lower confidence).
- "Combo kits" are the engine room of modern phishing. We found that 43.83% (3,780) of entries referenced multi-target lures - consistent with "panels" that impersonate many brands at once. That's how attackers scale: one kit, many victims, and many monetization paths.

- Attackers optimize for the fastest cash-out. Our analysis shows that single-target campaigns (1,952) heavily favor crypto (53.9% of single-target) and Microsoft/O365 (21.37%) for a high payoff, repeatable access.
- Multi-target kits overwhelmingly feature banking (81.86% of multi-target rows) plus e-commerce (76.39%) and PayPal (75.08%) - the "fraud trifecta" for consumer monetization.
- The ecosystem is global, collaborative, and multilingual - but concentrated. English dominates (~77%), while Russian is smaller in volume (~5%) but high-value for serious underground tradecraft (though it could be that this conclusion stems from our biased execution of this research). The net effect: threats can be built in one region, sold in another, and operated globally within hours.
- The barrier to entry keeps dropping. "Scama" bundles + tutorials + packaged infrastructure push phishing into a low-skill, high-impact category - more operators, more campaigns, more noise... and more successful compromises.

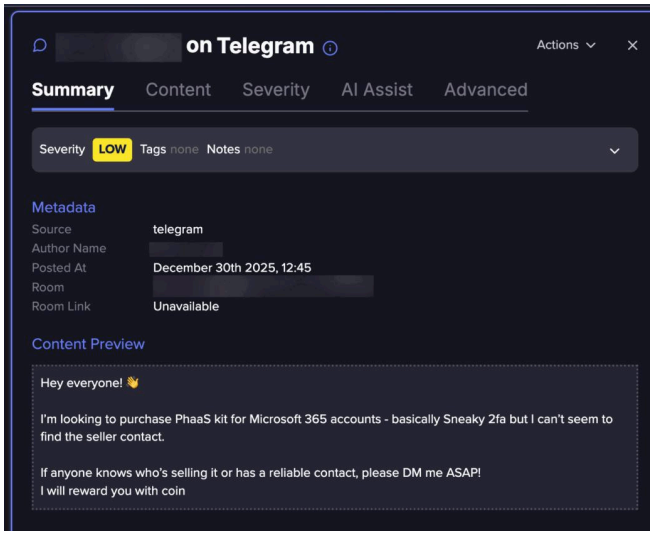
The State of Phishing in 2026

Phishing has crossed a line. In 2026, it no longer behaves like a social-engineering problem - it behaves like a mature underground industry with product lines, distribution channels, and constant R&D.

This research analyzed 8,627 distinct underground and adjacent posts tied to phishing kits, real-time phishing, and phishing-as-a-service. The signal is undeniable: 3,130 posts (36.3%) reflect high-confidence real threat activity, with another 20.5% showing suspected-real operational intent. In other words, phishing infrastructure isn't just "available" - it's actively traded, iterated, and deployed daily.

The data also explains why defenders are struggling. Modern kits increasingly revolve around AiTM and reverse-proxy capabilities that bypass OTP-based MFA, steal session cookies, and automate account takeover with minimal user suspicion. Meanwhile, "combo kits" dominate the market: 43.83% of posts reference multi-brand panels built to impersonate entire clusters of services in one deployment - with banking, e-commerce, and PayPal forming the core of mass-scale consumer fraud.

Most importantly, the market is evolving in ways that quietly break traditional controls. Hybrid kit ecosystems and Browser-in-the-Browser (BitB) deception are undermining legacy detections and awareness training ("check the URL") at the exact moment phishing is becoming cheaper, more automated, and more convincing.
This report dives into that economy - who builds these kits, how they're packaged and sold, which targets are prioritized, and what live phishing servers look like when they're actually operating — so defenders can shift from chasing indicators to disrupting behavior, infrastructure, and monetization workflows.



Threat actor on Telegram seeks out PhaaS kit
(Flare link to post, sign up for free trial to access if you aren't already a customer)

What is a “Phishing Kit”?

A phishing kit is a pre-packaged bundle of tools, scripts, and website templates that allows attackers to quickly deploy realistic phishing pages designed to steal passwords, session cookies, MFA tokens, credit-card details, or other sensitive data.

Instead of building an attack from scratch, these are the steps for a modern threat actor to execute an attack:

1. Simply upload the kit to a server (even those with limited technical skills)
2. Configure basic settings (like where stolen data should be sent)
3. Launch the campaign

Modern kits often include advanced features such as reverse proxy, real-time MFA bypass, dynamic logo replacement, bot detection, Telegram exfiltration, and automated victim tracking, making them one of the most widely used and scalable tools in the cybercrime ecosystem.

A newer evolution of this model is Phishing-as-a-Service (PhaaS), where operators sell subscriptions to ready-made phishing infrastructures, so customers never touch the underlying code. Such service often includes hosting services, lures, dashboards, and automatic updates. This turns phishing into a scalable, low-skill, high-impact service economy, dramatically increasing the volume and sophistication of global phishing campaigns. This evolution effectively turns the underground economy into a mirror of the legitimate market (what we call the “cybercrime assembly line”), where the “products” are technical services and illicit data. Each actor specializes according to their capabilities: tech savvy individuals build the tools, service operators run the infrastructure, and attackers simply purchase what they need - targeting lists, phishing infrastructure, or turnkey exploitation services.

As a result, many actors no longer conduct full campaigns themselves; instead, they buy services, execute small portions of the kill chain, and trade only the deliverables: Namely valid access to compromised accounts, websites, and entire organizations.

Research Methodology: Initial Underground Markets Datasets

We gathered a dataset of 8,859 entries from the past year with mentions of “phishing kits,” “phish kits,” and “real-time phishing.”

We identified 232 exact duplicate entries (2.7% of the data) which were removed, yielding 8,627 distinct posts for analysis. This cleaning step reduced noise and prevented double-counting in subsequent statistics.
Each entry’s textual fields – including any content, message, title, or description – were concatenated into a unified text field. This ensured that indicators (like kit names or keywords) scattered across different fields would be caught in analysis.

We further categorized the dataset along several dimensions: the source type, the actor typology, and the content type. This multi-dimensional approach reveals what kind of sources we’re dealing with, who the threat actors are (in terms of role), and what exactly they are doing or offering.

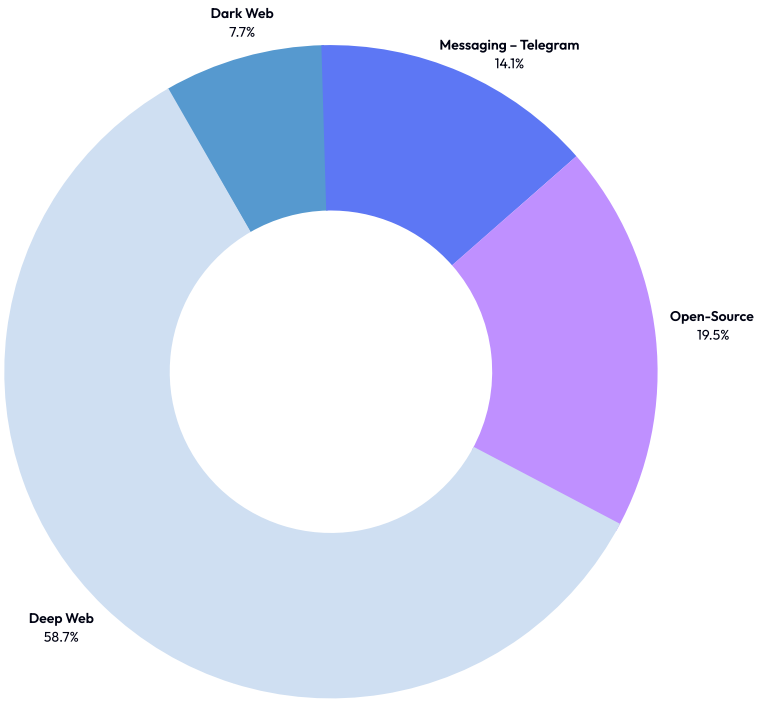
Source Type: Open-Source vs Deep vs Dark Web

We tagged each post as originating from open-source, messaging platform, deep web, or dark web:

- **Deep Web (58.8%):** Restricted or unindexed platforms on the clear web. The bulk of data came from login-only forums and invite communities (carding forums like CrdPro, cracking forums like Cracked/Nulled). These are not publicly indexed, but also not on Tor - one needs membership or specific links to access them.
- **Open-Source (19.4%):** Publicly accessible sites and feeds. This included cybersecurity news sites (e.g. Red Hot Cyber, Malware News blogs) and code platforms like GitHub/Gist. Paste sites and clear web social media (if any) would fall here as well. Essentially, no special access needed.
- **Messaging Platforms - Telegram (14.1%):** Semi-closed, invitation-based messaging ecosystems operating on the open source. Telegram channels and group chats act as high-velocity distribution hubs for leaks, malware announcements, phishing kits, stealer logs, and service advertisements. These environments are not publicly indexed, and while not part of the Tor darknet, they function as ephemeral micro-markets where threat actors, scammers, brokers, and automated bots push real-time updates.
- **Dark Web (7.7%):** Content explicitly on Tor/.onion or similar darknets. Notable dark web sources in the data included the Dread forum (a Tor forum) and certain darknet marketplaces or leak sites (e.g. posts from a "Carder Market" .onion, and others with .onion URLs). Only a minority of items were from purely dark web sites.

Source Environment Breakdown

The dominance of deep-web sources reflects that many threat actors congregate on closed forums and encrypted chat channels, while pure dark web markets/forums made up a smaller portion of this particular collection. Open-source references comprised roughly one-fifth of the data – largely due to numerous news articles being captured from OSINT feeds.



Posts by Source Type: The majority of posts originated from closed deep web forums, with a smaller fraction from open sources and a minority from Tor-hidden sites.

Targets Analysis: Targeted Organizations Breakdown

Out of the 8,627 total posts, messages and threads analyzed, the dataset naturally breaks into three mutually exclusive groups that together account for 100% of all entries:

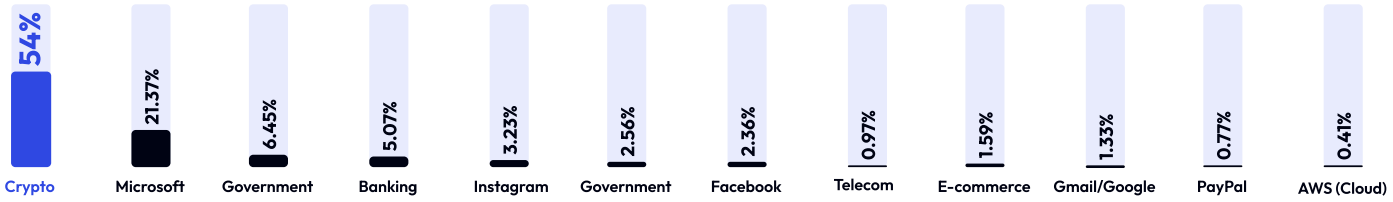
1. **No Target Identified (2,895 entries - 33.56%):** contained no recognizable target, representing generic chatter, low-signal posts, or content not tied to a specific brand or service.
2. **A Single Target (1,952 entries - 22.61%):** were single-target rows, where exactly one brand or sector was mentioned - typically focused phishing attempts such as crypto-only or Microsoft-only campaigns.
3. **Multi-targets (3,780 entries - 43.83%):** were multi-target rows, where two or more brands appeared together, which is characteristic of combo phishing kits and multi-brand scam packages that simultaneously impersonate banks, e-commerce platforms, payment processors, and identity providers.

Below you can see further analysis of the 1,952 (22.61%) single-target campaigns:

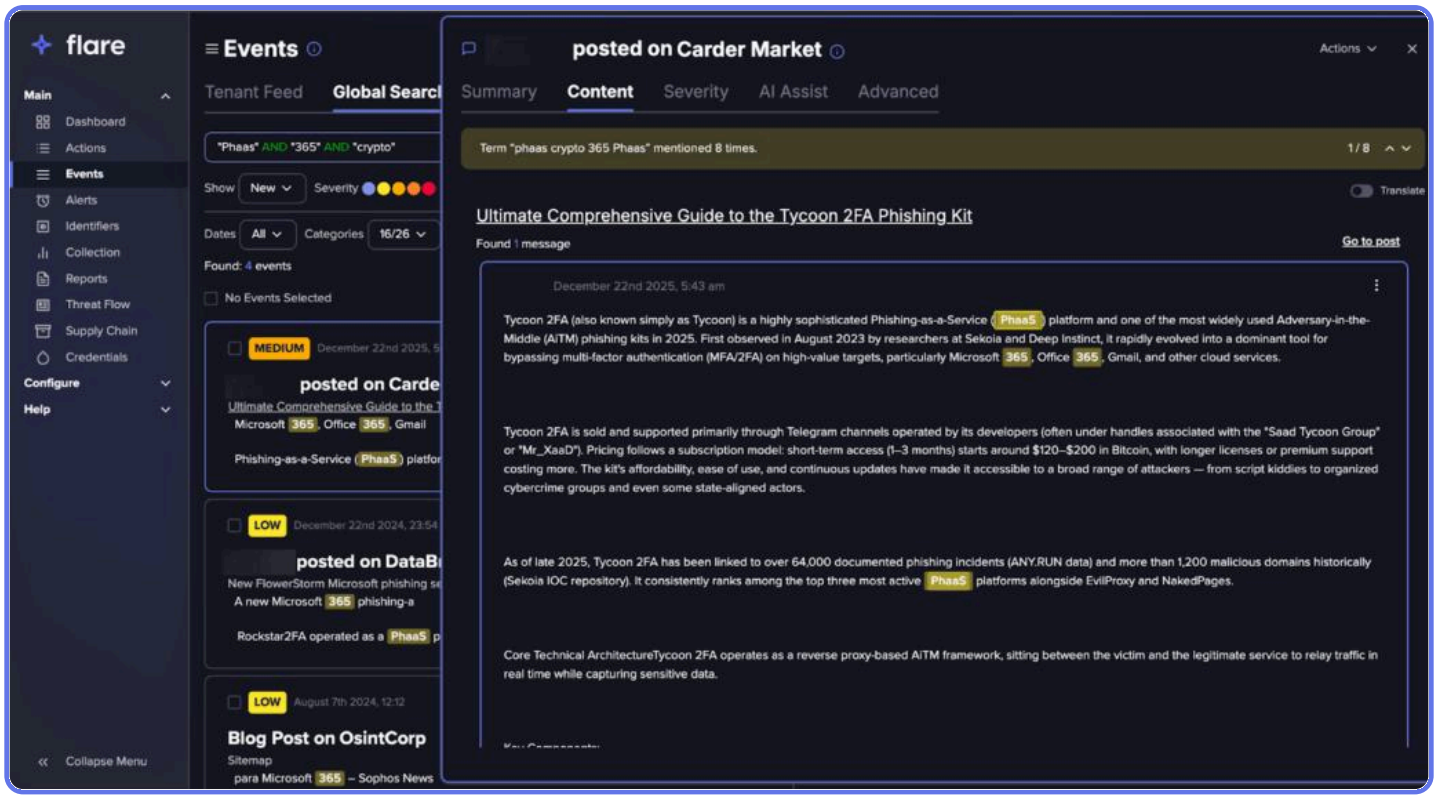
Target	Count	% of All (8,627)	% of Category (1,952)	Sector
Crypto	**1,052**	**12.19%**	**53.90%**	**Crypto**
Microsoft	417	4.83%	21.37%	Enterprise SaaS
Apple/iCloud	126	1.46%	6.45%	Consumer tech
Banking	99	1.15%	5.07%	Financial
Instagram	63	0.73%	3.23%	Social media
Government	50	0.58%	2.56%	Public sector
Facebook	46	0.53%	2.36%	Social media
Telecom	19	0.22%	0.97%	Telecom
E-commerce	31	0.36%	1.59%	E-commerce
Gmail/Google	26	0.30%	1.33%	Identity email
PayPal	15	0.17%	0.77%	Payments
AWS (Cloud)	8	0.09%	0.41%	Cloud computing

A few patterns jump out immediately:

- **Crypto dominates:** Over half (54%) of all single-target posts are crypto-only attacks. This suggests dedicated operations focused on stealing wallet seeds, exchange credentials, or private keys - high reward, low friction.



- **Microsoft-only:** These attacks come in second at 21%, reflecting the constant targeting of O365, Exchange, and enterprise identity systems. These are the bread-and-butter of BEC campaigns.
- **Everything else is niche:** Apple, banking, PayPal, social networks, and telecom providers make up only small fractions of single-target content. These brands appear far more often in multi-target phishing kits, where attackers load "combo kits" that impersonate multiple services at once.



Threat actor provides guide to Tycoon 2FA phishing kit on dark web market (Flare link to post, sign up for free trial to access if you aren't already a customer)

Single-target campaigns reveal the attackers' priorities. Crypto theft and corporate identity compromise are in the first place. Nearly all other impersonated brands only come into play when attackers run multi-target phishing kits, where they cast a wider net rather than aiming at one specific service.
This distinction is crucial for defenders.
Crypto and Microsoft ecosystems face the highest rate of deliberate, focused targeting - everything else is collateral in broader phishing operations.

While single-target campaigns show us where attackers focus their energy, the multi-target rows reveal something even more important:

- the structure of combo phishing kits
- all-in-one scam panels
- turnkey criminal tools designed to impersonate many brands at once

Below you can observe the analysis of 3,780 entries (43.83%) mention two or more target categories:

Target in Multi-Target Rows	Count	% of All (8,627)	% of Multi (3,780)	Sector
Banking	3,094	35.85%	81.86%	Financial
E-commerce	2,888	33.48%	76.39%	E-commerce
PayPal	2,839	32.90%	75.08%	Payments
Gmail/Google	760	8.81%	20.10%	Identity/email
Crypto	746	8.65%	19.73%	Crypto/Web3
Microsoft	628	7.28%	16.61%	Enterprise/SaaS
Apple/iCloud	483	5.60%	12.78%	Consumer tech
Government	376	4.36%	9.94%	Public sector
Facebook	405	4.69%	10.71%	Social media
Telecom	247	2.86%	6.53%	Telecom
Instagram	223	2.58%	5.90%	Social media
AWS (Cloud)	120	1.39%	3.17%	Cloud computing

Multi-target rows represent the **engine room of modern phishing** - the kits, templates, and scam pages attackers rely on to impersonate many different services at once.

Several strong patterns emerge:

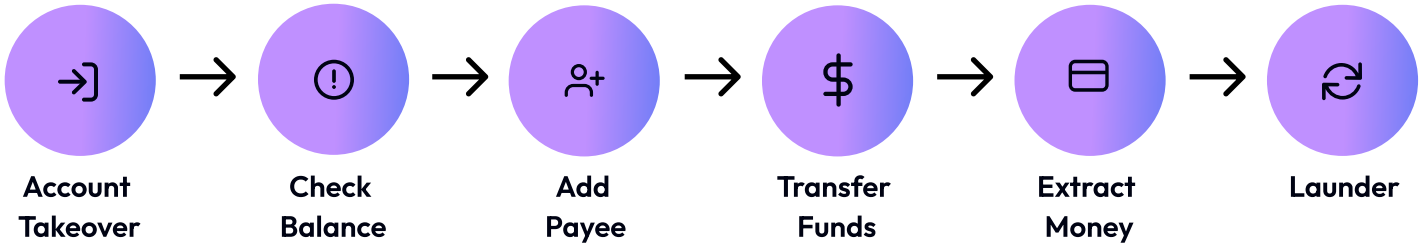
- Banking is the backbone of multi-target kits (82%): Almost every major phishing panel includes at least one bank. This reflects how scam kits are structured: actors bundle several banks together so a single landing page can adapt to whichever brand the victim expects.
- The “fraud trifecta”is e-commerce + PayPal + banking: With e-commerce at 76% and PayPal at 75%, these two appear consistently alongside banking targets. Typical combo workflow:
“Choose your target → Choose your bank → Enter your e-commerce or PayPal credentials → Hand over identity/email recovery info.”

- This is mass-market consumer fraud, optimized for scale.
- Identity providers (Google, Microsoft, Apple) act as “supporting targets”: Notice these brands appear much more in multi-target rows than single-target rows. They are the enablers of account takeover, not usually the final objective.

The Phishing Ecosystem Looks a Lot Like Legal Businesses

Phishing-driven cybercrime in the underground economy mirrors a rational market shaped by target preference, expected yield, and ease of monetization. Across thousands of posts, tools, and discussions, banks, financial services, and e-commerce platforms consistently dominate as the most targeted, most traded, and most talked-about sectors. The reason is simple: they offer the fastest and most direct path to cash-out.

For banking targets, the workflow is straightforward:



Other categories, such as identity providers or enterprise SaaS platforms, offer a less immediate or less predictable financial return. Fewer threat actors operate in those areas, and the cybercrime market shows lower liquidity and lower willingness to trade such access. These markets exist - but they behave more like specialized niches, not mass-market commodities.

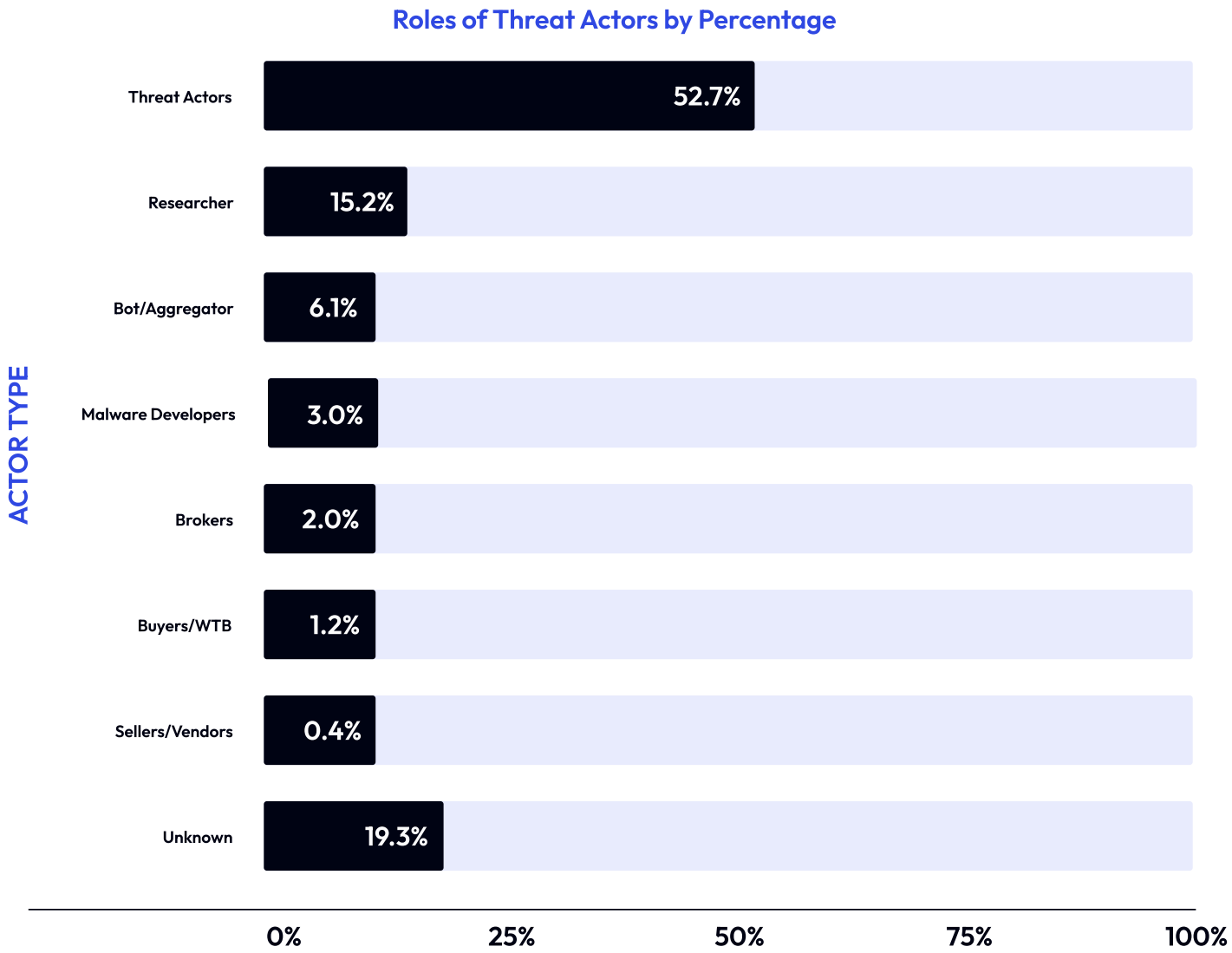
On the supply side, phishing kit developers respond to this demand by creating combo kits that impersonate banks, PayPal, e-commerce, and email providers simultaneously. This expands the customer base while minimizing development effort. Once again, despite being labeled “black market” or “underground,” the ecosystem behaves exactly like a rational economic system - governed by supply, demand, efficiency, and commodification.

Actor Typology: Roles of Threat Actors

We categorized the actors (authors or posters) into several persona/role types, based on their behavior and content:

- **Threat Actors (52.7%):** This was the largest category, encompassing actors engaging in or facilitating illicit activities without a specific niche like selling or buying. It includes forum members sharing or requesting hacking tactics, bragging about breaches, or dropping leaked data. Many posts on hacking forums fell here by default (e.g. a user discussing how to conduct a phishing campaign would be a generic threat actor).

- **Researcher (15.2%):** Actors sharing research, analysis, or otherwise acting in an OSINT capacity rather than criminal. This includes blog authors and OSINT analysts. Many OSINT blog posts (e.g. from RedHotCyber or OsintCorp) were attributed to this category. These entries, while found on underground forums or channels, are actually written by cybersecurity professionals or journalists (and often reposted by bots).
- **Bot/Aggregator (6.1%)**: Automated accounts that post content like news or breach data in bulk. About 530 posts came from such bots. For instance, the **"The Latest News"** account on Hydra forum that regularly posted cybersecurity news articles is considered an aggregator bot. Similarly, a Telegram channel named "Malware News" that reposts blog content would be a bot account. They are not human threat actors, but their posts populate many forums with intel or news.
- **Malware Developers (3.0%):** Actors showcasing technical skills or code, likely the creators of malware or exploit tools. ~260 posts fit this role. These often came from code-sharing (like GitHub) or forum posts with snippets of exploit code, developers advertising their custom malware, etc. For example, a user sharing a custom **stealer malware source code** or discussing development of a phishing page would be put here.
- **Brokers (2.0%):** Intermediaries or actors offering to connect buyers and sellers, or offering **insider access** and brokering deals. We flagged 170 posts as brokers – for example, posts that mention having "insider contacts" or facilitating sales of network access could imply a broker role. One pattern was posts offering **corporate insider information or access** (selling access into companies via employees) – those actors function as access brokers in the ecosystem.
- **Sellers/Vendors (0.4%):** Actors explicitly offering goods or services for sale. Surprisingly few posts (just 33) were clearly marked as vendor listings in our data. This is because many sales happen in replies or are implied; only certain marketplaces or "Sellers" sections had structured listings with **price** tags. Still, we did identify some, such as marketplace posts with a price field or posts in "Sellers" subforums (like BreachForums > Marketplace > Sellers Place).
- **Buyers/WTB (1.2%):** Actors looking to buy illicit products or access ("WTB" = Want To Buy). For instance, posts in Buyers sections of markets or requests like "I am looking for XYZ data, willing to pay" were classified as buyers. These were relatively rare (just 101 instances) – indicating demand is often communicated privately or that our collection focused more on offers than requests.
- **Unknown (19.3%):** In cases where we could not infer the role, we left the actor typology as Unknown. This often happened with short or context-less posts. For example, a one-line post saying "Selling method DM me" without clarity if the poster is a serious vendor or just scamming might be unknown. About one in five posts were ambiguous in this way.

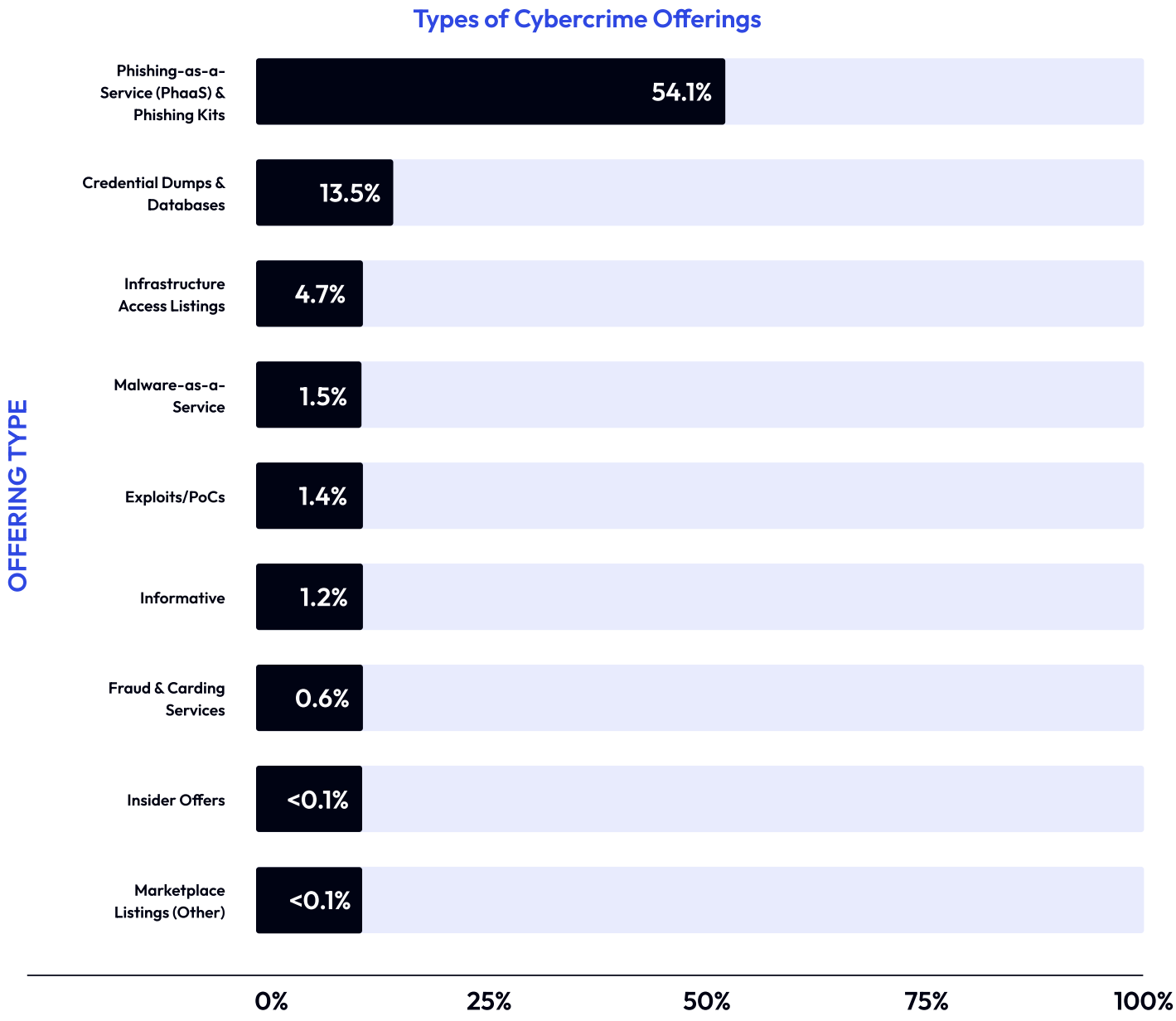


The prevalence of Threat Actor as a category underscores that a large portion of the content involves general malicious chatter and activity (not explicitly transactional). This mix of actors highlights a converged threat ecosystem where you have genuine criminals, scam artists, and OSINT feeds all posting in overlapping channels.

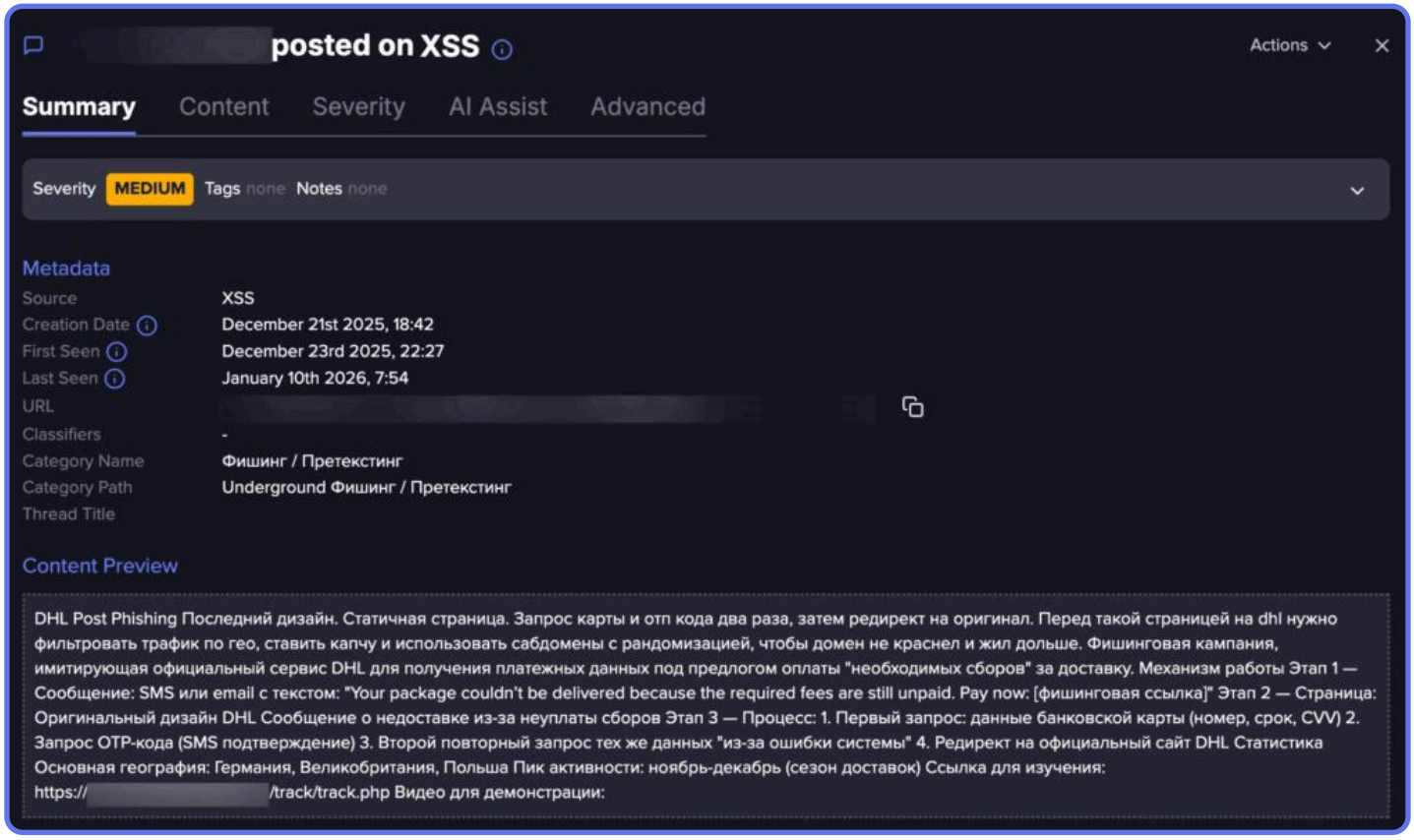
Content Type: Threat Services and Offerings

While all collected items contained at least one of our target search terms (most notably “phishing kits”) the actual subject matter frequently diverged. Many posts matched the keyword mechanically but discussed different themes altogether. We categorized what the content was about, focusing on the nature of the threat or product discussed. Key content-type categories identified:

- **Phishing-as-a-Service (PhaaS) & Phishing Kits (54.1%):** By far the largest chunk of posts involved phishing tools and services. This includes discussions or sales of phishing kits (like reverse-proxy kits to bypass 2FA), references to PhaaS platforms, and related tactics. The prominence is due in part to our collection criteria (which targeted these terms) - nonetheless, it underscores that phishing kits are a hot topic in 2025. Posts ranged from technical analyses of kits (e.g. a news post on a new Sneaky 2FA kit using Browser-in-the-Browser tactics) to criminals actively seeking kits (as noted, a Dread user wanted to buy Astaroth's phishing kit) or sharing kit "config" files. Both open-source reporting and underground chatter show that advanced phishing kits (especially those defeating MFA) are a focal point.
- **Credential Dumps & Databases (13.5%):** Posts offering stolen credentials, email password combos, databases of user accounts, etc. These were often in "Leaks" or "Databases" sections of forums. For example, some forum threads provided download links to compromised credential lists or advertised fresh data breaches. This category (over 1,100 posts) indicates a thriving trade in credentials and data dumps on these platforms.
- **Infrastructure Access Listings (4.7%):** Offers or requests for hacked infrastructure - e.g. RDP servers, VPN credentials, webshell access, SMTP servers, or "bots" for use in further attacks. Around 408 posts fell here. These often appeared on marketplaces or in discussions about initial access. They represent the access broker economy (some posts explicitly advertised internal network access for sale).
- **Malware-as-a-Service (1.5%):** This includes anything where malware or hacking capability is offered as a service (apart from phishing kits). For instance, ransomware-as-a-service (RaaS) ads, crypter and botnet rentals, stealer log marketplaces, etc. We flagged ~132 posts, such as those selling stealer logs (our data even had a source called "potential_stealer_logs") or advertising DDoS botnets. While present, this was a smaller slice compared to phishing – suggesting the current underground chatter leans more to credential/phishing operations than classic malware.
- **Exploits/PoCs (1.4%):** Posts sharing proof-of-concept code or exploits for vulnerabilities. There were ~118 such posts. For example, a GitHub gist containing a PoC for a CVE, or a forum user posting an exploit script in a code block. These indicate some actors (or researchers) sharing offensive tools, which could be used by others.
- **Fraud & Carding Services (0.6%):** Offers related to payment fraud, fake documents, credit card data, and the like. Only ~52 posts were explicitly in this vein (possibly because our collection was more phishing-focused). Still, we saw content like tutorials on "carding methods" or vendors for fake IDs and bank drops. These are part of the broader cybercrime economy but were a minor part of this dataset.
- **Insider Offers (<0.1%):** Only two posts were tagged here, showing it's quite rare explicitly in our set. These would be instances of someone claiming insider access or recruiting an insider at a target organization. It's a niche but highly dangerous content type – essentially facilitating corporate espionage. The low count doesn't mean it's unimportant, just that it wasn't common in the scraped sources.
- **Marketplace Listings (Other) (<0.1%):** A handful of sale posts that didn't fit neatly in the above categories (only six entries). These might be listings for miscellaneous items or services on underground markets (e.g. illicit "keys" or accounts that are not credentials but digital goods).
- **Informative (1.2%):** Posts that were informative reports or articles rather than offers. (Most OSINT articles were still about phishing kits hence counted in PhaaS category, but about 106 were more general news not focusing on those kit keywords). These include industry reports shared on forums (e.g. an analysis of an APT operation). They are included for completeness but are not actor-driven content.



Overall, the content landscape is heavily skewed toward phishing kits and credential theft services. This aligns with current threat trends – phishing kits are a major commodity. In fact, one report noted that the Tycoon2FA kit (one of the kits frequently mentioned in our data) was responsible for almost 90% of recent PhaaS incidents, showing how one or two popular kits dominate. Our data reflects this dominance: references to Tycoon2FA and its ilk were widespread.



A Russian speaking threat actor posts an advertise about a DHL phishing kit, this is part of a broader discourse in Russian, with many live examples of phishing kits (Flare link to post, sign up for free trial to access if you aren't already a customer)

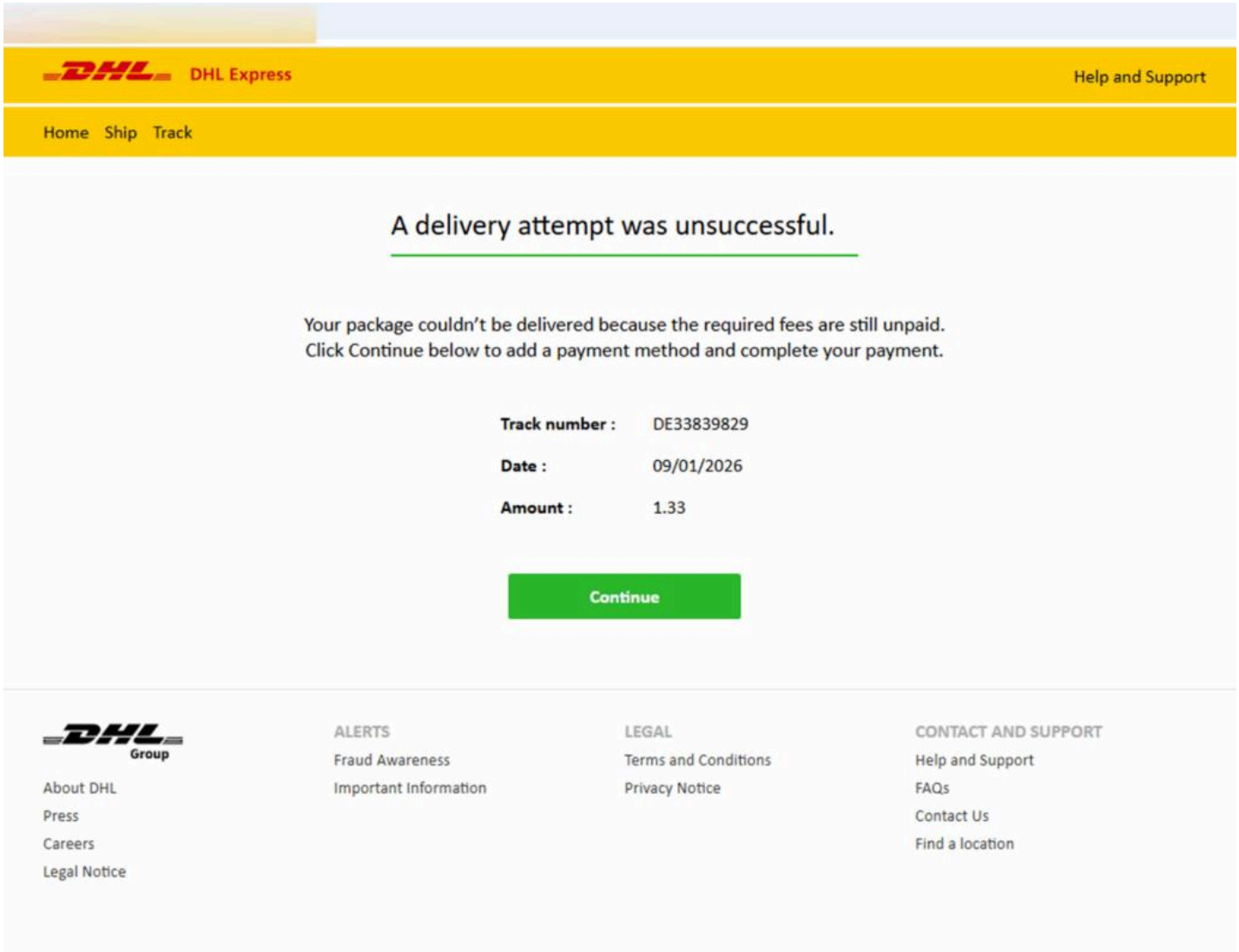
Post translation:

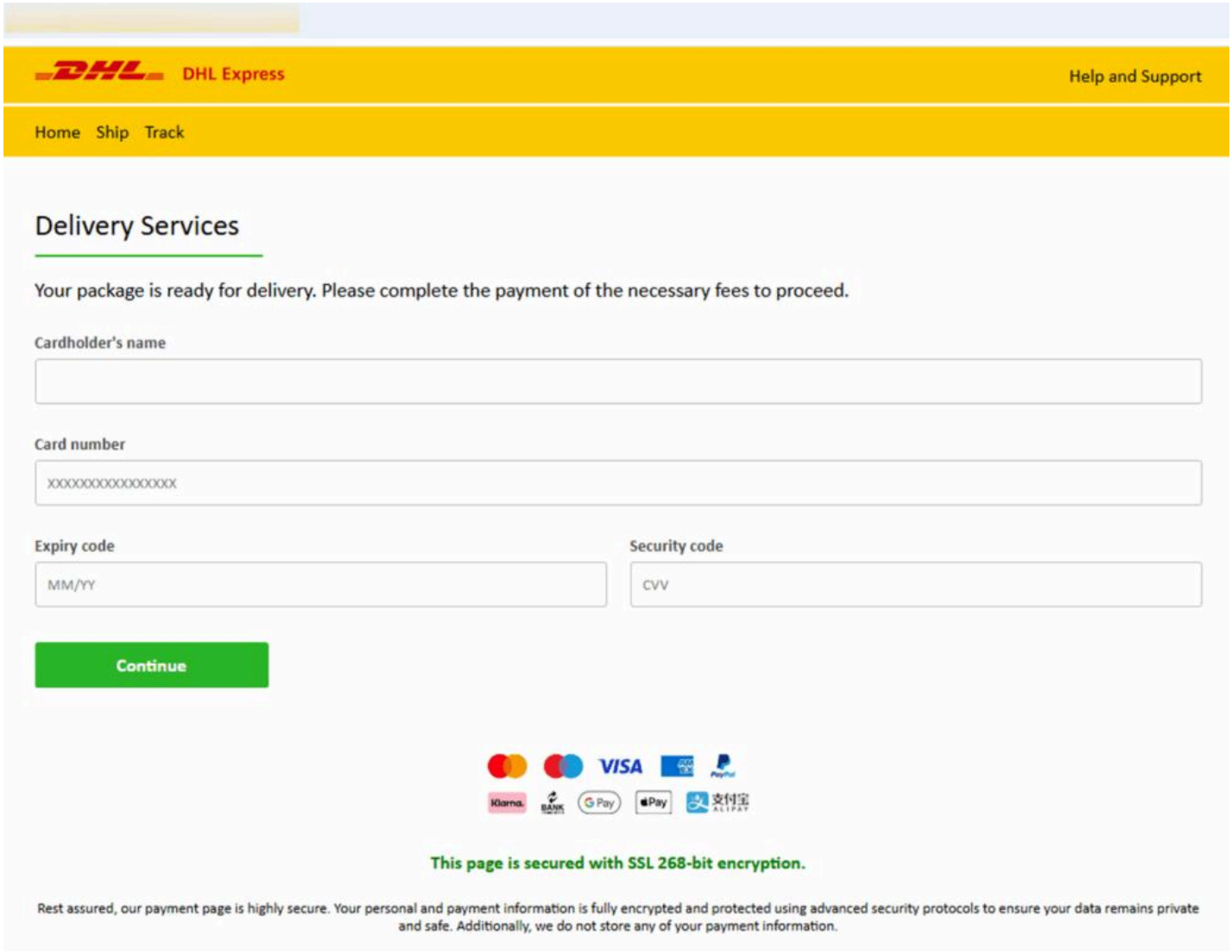
> DHL Post Phishing.
>
> Latest design.
>
> Static page.
>
> Requests a card and OTP code twice, then redirects to the original. Before such a page on DHL, you should filter traffic by geo, set a captcha, and use randomized subdomains to prevent the domain from being flagged and extend its lifespan.
>
> A phishing campaign imitating the official DHL service to obtain payment information under the pretext of paying "required fees" for delivery.

How it works:

1. Step 1 - Message: SMS or email with the text: "Your package couldn't be delivered because the required fees are still unpaid. Pay now: [phishing link]"
2. Step 2 - Page: Original DHL design Message about non-delivery due to non-payment of fees
3. Step 3 - Process:
    a. First request: bank card details (number, expiration date, CVV)
    b. Request for OTP code (SMS confirmation)
    c. Second repeat request for the same details "due to a system error"
    d. Redirect to the official DHL website Statistics Main geography: Germany, UK, Poland

Peak activity: November-December (delivery season)
Link for study: https://<redacted>/track/track.php





Screenshots from fake DHL pages

Notable Products, Kits, and Campaigns Trends

The discussion gravitates toward a diverse set of tool families, hybridized kits, emerging 2FA-bypass methods, and evolving attacker tradecraft. Below is a consolidated analysis of the most prominent kit families, their relationships, and the operational trends shaping the phishing landscape.

- **EvilProxy (334 entries):** EvilProxy remains the most frequently referenced phishing kit in the dataset. As a mature 2FA-bypassing reverse-proxy platform with an established affiliate ecosystem, EvilProxy appeared in both threat-actor conversations and security research reports. Its widespread use demonstrates its central role in modern AiTM phishing, targeting Google, Microsoft, developer platforms, and more. At least 145 distinct actors referenced EvilProxy, underscoring its deep penetration into the underground market.

- **Tycoon2FA (240 entries):** Tycoon2FA emerges as one of the most strategically significant kits in 2025. Often discussed alongside the older Salty2FA kit, recent research shows that the two have effectively merged into a hybrid "chimera" platform. As Salty2FA's infrastructure degraded in late 2025, it began quietly failing over to Tycoon2FA's backend, reviving Salty's capabilities under a new umbrella. This evolution explains why Salty2FA-only activity collapsed from hundreds per week to just a handful while Tycoon2FA detections surged. The hybrid kit is increasingly evading legacy detection signatures.
- **Scama (45 entries):** The term "scama" is derived from "scam page" and popularized by Vade researchers. It is used primarily in OSINT and threat-intel reporting, not by criminals themselves. Only four unique actors used the term, indicating it is not native to underground communities. Scama refers to complete phishing "packs" with templates, SMS spam modules, responsive design, and turnkey deployment features that lower the barrier to entry for inexperienced attackers.
- **Browser-in-the-Browser (BitB) (154 entries):** BitB is not a kit but a powerful technique leveraged by multiple phishing frameworks. It creates a fake browser window (complete with spoofed URL bar) allowing attackers to bypass user intuition and security awareness training. BitB frequently appears alongside EvilProxy and Sneaky2FA, including 43 posts discussing EvilProxy + BitB together. BitB has become a standard feature in next-generation phishing kits.
- **Other Notable Kits:**
  - **Sneaky2FA (21 entries):** A BitB-enabled kit enabling pixel-perfect fake login windows; highlighted by Malwarebytes for targeting Microsoft accounts.
  - **Salty2FA (18 entries):** Now mostly absorbed into the Tycoon2FA hybrid infrastructure.
  - **Whisper 2FA (4 entries):** A newly emerging AiTM kit reportedly linked to over one million phishing attempts in just a few months. Indicating rapid adoption potential.

Analysis of co-mentions reveals meaningful structural relationships across kit ecosystems:

- **EvilProxy + BitB:** Mentioned together in 43 posts, which reflects how BitB is increasingly tied to advanced AiTM campaigns.
- **Tycoon2FA + EvilProxy:** Co-mentioned 32 times, typically in comparisons of leading phishing-as-a-service (PhaaS) platforms.
- **Tycoon2FA + Salty2FA:** Strong correlation due to hybridization; joint mentions track the collapse of Salty's standalone presence.
- **Tycoon2FA + BitB:** Appeared together 11 times, indicating discussion of Tycoon-like kits adopting BitB-style deception.
- **Scama:** Rarely overlaps with the above families, further demonstrating that it is a researcher classification rather than an attacker-operated brand.

These co-occurrence patterns show that modern phishing discussions often center not on individual tools but on broader attacker workflows, such as AiTM proxies, BitB deception layers, and multi-kit hybrid infrastructures.

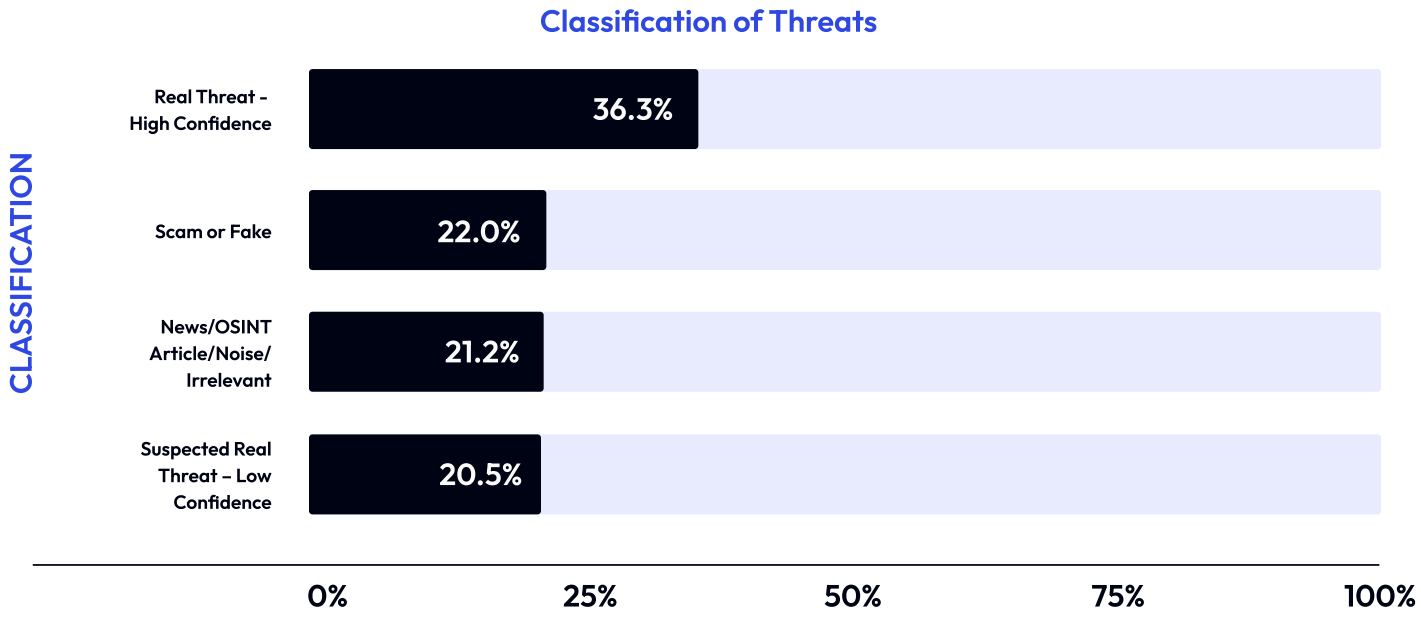
1. **Tycoon–Salty Hybrid Campaign:** The fusion of Tycoon2FA and Salty2FA represents a pivotal development. The hybrid kit is likely responsible for the resurgence of 2FA-bypass campaigns in late 2025. The campaign demonstrates:
    - seamless failover between backend infrastructures
    - increased resilience against takedowns
    - rising detection evasion
2. **EvilProxy's Distributed Campaign Footprint:** Rather than one large campaign, EvilProxy acts as a platform powering countless smaller attacks. Its widespread use by many actors, combined with constant feature updates, makes it a long-term strategic threat.
3. **Sneaky2FA & BitB Social Engineering Campaigns**: Sneaky2FA demonstrates that **front-end deception** (pixel-perfect fake login UIs) is becoming as critical to phishing success as backend infrastructure. These campaigns are effective even against well-trained corporate users.
4. **Whisper 2FA's Rapid-Scale Campaigns:** Early analysis suggests Whisper 2FA may become the next major AiTM platform. Its reported operational scale (over one million attempts) indicates high automation and probable service-based distribution.
5. **Telegram-Integrated Real-Time Phishing:** Some campaigns incorporate Telegram OTP bots that coordinate live interaction with victims (voice call social engineering, OTP harvesting, etc.). These bots act as **automation bridges** between phishing kits and social-engineering operations.
6. **AI-Assisted Phishing:** Some posts discuss using LLMs to generate phishing pages, emails, or even code. This trend anticipates a coming wave of **hyper-polished, auto-localized phishing operations** where AI handles crafting, interaction, and adaptation at scale.

Authenticity & Confidence Assessment

Each post was systematically evaluated for authenticity and assigned both an authenticity tier and a confidence level. To ensure clarity and analytical consistency, every item in the dataset was classified into one of five high-level categories, reflecting its nature, intent, and relevance to real-world malicious activity:

- **Real Threat - High Confidence (3,130 entries - 36.3%):** Posts considered genuine, actionable threat activity with high confidence. These include credible offers of illicit data or access, and discussions by known threat actors. Posts on established underground forums (Exploit, XSS, BreachForums, etc.) or by reputable threat actors generally fell in this category. For example, a dark web reputable forum post by an active user seeking to purchase a high-end phishing kit (priced at $2,000).
- **Suspected Real Threat - Low Confidence (1,769 entries - 20.5%):** Posts considered likely malicious, not fully verified, ambiguous actors, and/or new channels. The content looks genuine and the threat actors look real, but we don't have enough evidence or the data is inconclusive to rule that this is a genuine threat with high confidence. This includes discussion threads about hacking techniques, offers of malicious services that seem plausible but unconfirmed, etc. For instance, a Dread forum user asking for "realistic methods" to conduct hacks (avoiding "script kiddie" ideas) is operational content - malicious in intent but not an outright confirmed breach.

- **Scam or Fake (1,898 entries - 22.0%):** Posts that were assessed as likely fraudulent, illegitimate, or very low-quality. Common signs included too-good-to-be-true hacking services, zero reputation sellers, and copy-paste ads. A prime example is a Telegram message listing dozens of hacking services (from spy apps to "SIM swapping as a service" to "AI-Based Social Engineering").
- **News/OSINT Article/Noise/Irrelevant (1,830 entries - 21.2%):** Open-source reports, threat intel blog posts, and news articles shared within forums. For example, many Hydra forum posts were simply copied news articles from sites like CSO or TheCyberExpress. Alternatively, content unrelated to threats or otherwise useless for CTI. Only 29 entries fell here (e.g. blank posts, test messages, or trivial one-liners like "thanks" and "cool" with no intel value). These were filtered out from most analyses.



High-confidence real threats typically appeared on established cybercrime platforms and included concrete operational details (such as data samples, pricing, or actor contact channels) that strongly signaled authenticity. Scam posts, by contrast, were generic, exaggerated, or implausible.

A clear example is the EncryptedByNinja ad, which claimed "12+ years' experience" and offered everything from credential stuffing to "Critical Infrastructure Attacks" in a single pitch - classic hallmarks of a fake service.

News articles were easy to identify by their formatting, source references, and frequent reposting by bot accounts like The Latest News. Posts classified as "Suspected Real" tended to be operational but unverified - vague access sales, requests for illicit services, or offers lacking proof or reputation signals.

Each entry also received a confidence score reflecting how certain we were in its classification. High confidence was applied to clearly real threats, confirmed scams, and OSINT/news content whose nature was unambiguous. Medium confidence covered the operational-but-unconfirmed middle ground. No posts required a "Low" confidence label. Anything too uncertain defaulted to Medium. Ultimately, about 79% of the dataset received High confidence and 21% Medium, indicating that the majority of posts could be reliably assessed based on context cues and platform credibility.

Language Segmentation Analysis

The dataset's multilingual nature provides insight into geographical targeting and community segmentation:

- English (Latin script) – ~77%: As noted, English dominated the content. This includes both international forums (many forums, even if they cater to global audiences, use English as a common tongue) and English-language reporting. The high English ratio also comes from Telegram groups, many of which operate in English or broken English (even if actors are non-native). For real threat content specifically, English posts encompassed everything from English-speaking criminal forums to global leak announcements. Essentially, English is the lingua franca of cybercrime in a lot of contexts, especially for phishing and fraud.
- Russian (Cyrillic) – ~5%: The Russian content, while a smaller portion of total posts, is very important qualitatively. Russian forums like Exploit and XSS are known for technical sophistication and significant breaches. In our high-confidence threat subset, Russian probably accounts for ~15% (since none of the OSINT news are Russian, Russian language's share grows when focusing on just threats). These Russian posts were mostly related to carding, hacking tutorials, and malware. For example, posts about payment systems and BINs in Russian. They were not discussing the likes of Tycoon2FA by name (since those kits are more associated with English-speaking services), but Russian actors have their own phishing frameworks. We should be aware that lack of explicit kit names in Russian text doesn't mean lack of phishing activity – it might be described differently.
- Italian – ~15%: All Italian entries were from the Red Hot Cyber news feed. They covered a broad array of topics (phishing kits, cyber policy, etc.) but are not threat actor posts. When analyzing "real threats," Italian essentially drops to 0%. However, this segment is important for context and shows the presence of regional cyber news. It also suggests that Italian organizations are curating CTI content (since Red Hot Cyber is an Italian source), possibly indicating interest in these threats in Southern Europe. For our purposes, Italian content was an OSINT lens on primarily English/Russian threats.
- Spanish – ~0.25%: A very small number of posts were in Spanish. Those that were, came from the Underc0de forum (which is a Spanish-language hacking forum) and a few OSINT pieces. The Spanish forum posts included things like general hacking news or tips, not major criminal transactions. In the high-confidence threat realm, Spanish content was negligible – serious actors in Spanish tend to either join English forums or remain in smaller communities (which were not extensively captured here). Nonetheless, Spanish-speaking threat actors exist (Latin American financial fraud rings, etc.), so the minimal Spanish in our data might indicate under-collection rather than absence of threats. It might be worth adding more sources targeting Spanish cybercrime forums in the future.
- Portuguese – ~0.27%: Similarly low presence. Possibly some content from Brazil or Portugal was captured via OSINT or paste sites. Brazil has a known underground (e.g. Red Hot Cyber often covers Brazilian cyber news on their Portuguese site), but our dataset seems to have only a handful of Portuguese items. These could be references or maybe a snippet from a Lusophone forum. For now, Portuguese posts didn't contribute meaningfully to the real threat count. But Portuguese terms (for Brazilian banking malware etc.) could be relevant if focus shifts to that region.

- Arabic – ~0.09%: Just 8 posts. These likely came from an Arabic cybersecurity news channel (we saw a reference to “cybersecuritymiddleeast_bot”). They might have been translations or brief notes about threats in the Middle East. No significant Arabic dark web content was present. This indicates that while the Middle East has cyber activity, it wasn’t a focus in the collected data. If needed, monitoring Arabic-language cyber forums or Telegram groups (there are some related to hacking tools) could be expanded.
- Other Languages: Practically none aside from the above. No Chinese or Farsi or other Asian language content was directly in the dataset (only second-hand mentions via English sources). This again reflects our collection focus, but it also mirrors the reality that a lot of Chinese underground activity stays within Chinese platforms not scraped here, and similarly other languages might be siloed.

To summarize, English and Russian are the core languages one must cover for phishing/fraud threat intel. Italian in our data highlights OSINT reporting value. Spanish/Portuguese/Arabic content was minimal, suggesting either low representation or a need to tap into those communities better. For high-confidence threats, English remains dominant but Russian is absolutely vital to include because of the quality of intel from Russian forums (even if fewer in number, they often pertain to significant breaches or malware dev).

Cross-tabulating language with actor/content types shows that language often corresponds with different content focuses: e.g. Russian posts were frequently about carding or malware (since Russian forums excel in those topics), English posts covered the whole spectrum (phishing kits, leaks, etc.), and Italian covered summaries of all of the above (but not original criminal activity). Understanding this can help an analyst prioritize translation and monitoring efforts towards languages likely to yield the kinds of intel needed (e.g. translate Russian for breach data, ensure English sources for phishing kits, etc.).

Drafting a Threat Landscape Overview for 2026

The threat landscape reflected in these posts and instant messages reflects a phishing kits market that is gradually growing and increasing in its level of sophistication and market ready products. Phishing-as-a-Service platforms and ready-made phishing kits have become cornerstone tools for cybercriminals. The data shows a surge in discussion and usage of kits that can bypass multifactor authentication (MFA), indicating that even MFA-protected accounts are no longer safe. In addition, theft of session cookies, and DOM elements shows that the initial entry bar has been raised and the standard phishing kit isn’t just a lookalike scraped webpage with some sort of SSL. Kits like Tycoon2FA and EvilProxy are so prevalent that one or the other was referenced in the majority of collected intel posts. In fact, Tycoon2FA’s prolific use has been blamed for nearly 90% of recent phishing attacks that defeat MFA.

We see an arms race in play: as organizations adopt MFA, threat actors respond with reverse-proxy and browser-in-the-browser attacks. The emergence of hybrid kits (e.g. Salty2FA+Tycoon2FA merging) is a direct result of this evolution - threat actors are blending techniques to nullify single defenses. This has made detection and attribution harder, as noted by researchers: signature-based detection tuned to one kit can miss the hybrid. The implication is that defenders can no longer rely on static IoCs or kit-specific fingerprints; behavior-based detection (monitoring for things like odd login flows, “trampoline” pages, etc.) is now standard.

Another aspect of the landscape is commoditization. The term “Scama” encapsulates how phishing kits are being packaged and sold like off-the-shelf products, complete with customer support and add-ons. Virtually anyone willing to pay (sometimes as little as ~$20 on certain markets, or even free via underground YouTube tutorials) can obtain a professional-looking kit. These kits come with features like built-in email/SMS sending tools, blacklist checks, and tech support communities. This means the barrier to entry for phishing has dropped tremendously - an amateur can operate what was once the preserve of experienced hackers. Our data showed multiple newbie-oriented forums and channels where such kits are circulated.

The result is a flood of phishing campaigns, many targeting financial accounts, corporate email (for BEC), and more. For example, one report in our data highlighted a “Scanception” campaign using QR codes in phishing emails to evade detection, which resulted in 600+ phishing PDFs with 0 VirusTotal detections being circulated - evidence that these tools enable very stealthy attacks at scale.

It’s also worth noting the globalization of these threats: while many kit developers appear to be Russian or English-speaking, their services are used worldwide. We saw content about Middle Eastern phishing experiments (Sharjah Police’s QR code test) and references to Chinese phishing kit operations (the “Smishing Triad” using walls of phones for SMS phishing).

The kits often support multiple languages - one advertisement touted support for 43 languages in a scam page for maximum victim reach.

Thus, the landscape is one in which for example, a kit written by a Russian team, sold on a Tor forum, can be used by a cybercriminal in South Asia to phish a European company’s employees – a truly transnational threat scenario.

How Security Teams Can Defend Against the Rise of Phishing Kits

From this analysis, several actionable insights and hypotheses emerge:

1. **Prioritize Detection of MFA-Bypass Phishing:** Security teams should assume that phishing emails will bypass MFA via tools like EvilProxy. Implementing robust behavior-based detection is key. For instance, monitor for multiple login attempts in quick succession, or logins from cloud VMs (since these kits often run on cloud servers) - behaviors indicative of an AiTM proxy in action. Additionally, user education should emphasize that MFA prompts can be phished and encourage use of FIDO2 security keys or passkeys where possible (as those are harder to proxy).

2. **Targeted Threat Actor Monitoring:** Identify and monitor key individuals identified in this analysis (e.g. the top posters on certain forums, any actor who asked for or offered phishing kit capabilities). For example, a specific threat actor who posted 370 times on a carding forum and marked as highly credible is more likely to provide valuable info or link to other significant players. Monitor these key threat actors by creating watchlists for these handles and any associated contact info.

3. **Expand Language Coverage:** Given the findings, it's advisable to expand monitoring to Russian, Chinese and Farsi search terms. While the data corpus contains ample examples from these languages, in this research we only focused in English search terms. Our data corpus suggests Russian forums are active with high-tier threats, they appear very potent.
4. **Leverage OSINT to Augment Underground Intel:** The synergy of having OSINT articles alongside actor posts proved useful. For every major kit, researchers were putting out analysis (which we had in our data). Security practitioners can use those to inform what to look for in the raw actor chatter. For instance, Any.Run's report gave us specific behaviors of the Salty+Tycoon hybrid. We recommend reviewing any quiet period in phishing detection logs to see if that correlates with indicators of Tycoon2FA that maybe weren't flagged at the time.
5. **Defensive Training Adjustments:** The intelligence here about sophisticated phishing kits shows that user training must evolve. Telling users "check the URL bar" is no longer sufficient when kits can spoof the browser window convincingly. Security awareness programs should include examples of AiTM and BitB and advise things like "If an MFA prompt or login appears at an unusual time, be skeptical even if it looks normal." Also emphasize the use of password managers, since they can be a backstop against fake forms. To better train your organization against the latest phishing tricks (like QR code phishing, AiTM, BitB windows), incorporate them into phishing simulations for employees, to inoculate them somewhat and measure risk.

Monitor for Phishing Kits with Flare

The Flare Threat Exposure Management solution empowers organizations to proactively detect, prioritize, and mitigate the types of exposures commonly exploited by threat actors. Our platform automatically scans the clear & dark web and prominent threat actor communities 24/7 to discover unknown events, prioritize risks, and deliver actionable intelligence you can use instantly to improve security.

Flare integrates into your security program in 30 minutes and often replaces several SaaS and open source tools. See what external threats are exposed for your organization by signing up for our free trial.