2025 BERLIN

24 - 26 September, 2025 / Berlin, Germany

THE DARK PRESCRIPTION: INSIDE THE INFRASTRUCTURE OF ILLEGAL ONLINE PHARMACIES

Martin Chlumecký & Ľuboš Bever

Gen Digital, Czech Republic

martin.chlumecky@gendigital.com
lubos.bever@gendigital.com

ABSTRACT

The internet is flooded with fake pharmacies – over 95% of them operate illegally, selling everything from counterfeit medications to unapproved or prescription drugs. These operations don't just steal money or data – they put lives at risk. And behind the scenes, a sophisticated cybercriminal infrastructure is fuelling it all.

In this paper, we expose the hidden architecture that enables these global operations. By analysing network setups, payment gateways, code reuse, and advertising tactics, we connected thousands of fraudulent pharmacy sites to a single, well-organized cybercrime group. This actor exploits *Google* indexing, hijacks legitimate medical sites, and leverages public hosting to appear trustworthy – all while funnelling users through spam, adult content platforms, and even AI chatbot prompts.

The most aggressively pushed products? Drugs that people are desperate to get: erectile dysfunction medications, powerful antibiotics, and – increasingly – expensive and trendy weight loss treatments. The real cost? Compromised data, empty bank accounts, and in the worst cases, dangerous health consequences.

We'll walk through how this ecosystem works, how it hides in plain sight, and what the cybersecurity community can do to better detect and disrupt these digital drug lords – before more lives are put at risk.

INTRODUCTION

The growing presence of unlicensed online pharmacies poses a serious public health and digital security issue, making it essential to identify fake online pharmacies. These websites operate outside regulatory oversight, sell counterfeit, expired, or dangerous medications, and may be instruments for identity theft or financial fraud [1].

While pharmaceutical fraud is not a new phenomenon, the internet has become a productive ground for cybercriminals to exploit vulnerable consumers [2]. Today, it is estimated that up to 95% of online pharmacies operate illegally, offering prescription drugs without proper authorization or oversight [3].

Criminals often exploit moments of adverse health events – such as drug shortages or global crises like the COVID-19 pandemic – by offering false hope or hard-to-find medications. Prescription drugs and promising treatments are particularly targeted because desperate individuals seek quick and affordable access, often bypassing medical consultation.

The risks of using unverified or black-market medications are severe. These drugs may contain incorrect dosages, harmful contaminants, or be entirely ineffective. Safety, efficacy, or appropriate storage conditions are not guaranteed without proper regulation. This exposes users to toxicity, overdose, or dangerous side effects [4]. For example, medications for erectile dysfunction require thorough cardiovascular screening, for which a simple online form is no substitute.

The cynicism of these attackers extends beyond financial theft or data breaches – they directly threaten public health by distributing unsafe pharmaceuticals.

Problem statement

A growing number of online shops offer suspiciously cheap or prescription-only medications. Given that the sale of prescription drugs is strictly regulated in most countries, the legitimacy of these platforms is highly questionable.

Many fake pharmacies share remarkable similarities, such as nearly identical product ranges, the same payment methods, and a list of similar or identical contact information. Another common pattern is the use of trust-building elements meant to reassure visitors of the site's legitimacy. These patterns suggest a coordinated effort, possibly directed by a single threat actor or a tightly connected criminal network operating across borders.

It is alarming that fraudulent websites often appear among the top search results on popular search engines, which increases their visibility and reach. So, it raises urgent concerns about the scale and sophistication of the threat.

There is a crucial need to uncover the full area of this underground infrastructure, understand how it operates, how it reaches victims, and how it can be effectively disrupted.

This paper comprehensively investigates the hidden infrastructure behind illegal online pharmacies by uncovering evidence of a coordinated cybercriminal operation. Through technical analysis, we examine the infrastructure, tactics, and recurring patterns that link seemingly disparate pharmacy websites.

Additionally, we provide practical recommendations for identifying suspicious platforms and protecting users from falling victim to these schemes. Ultimately, this paper seeks to raise awareness among internet users and cybersecurity professionals about the growing threat of fake online pharmacies and the urgent need for collective action to combat it.

OVERVIEW OF THE ONLINE PHARMACY ECOSYSTEM

Online pharmacies offer convenience worldwide, but regulations vary by country. Legitimate sites must provide full contact details and be registered with national authorities, such as the FDA (US), BfArM (Germany), or SÚKL (Czech Republic).

In the European Union, online pharmacies must display a specific logo (see Figure 1) that links to the national regulatory authority's website. This allows users to verify the pharmacy's legitimacy directly. These measures are designed to protect consumers from counterfeit or unsafe medications.

Figure 1: European Union-certified online pharmacy badge indicating compliance with EU regulations.

In the United States, online prescription drug sales are more common, but strictly regulated. The FDA and the National Association of Boards of Pharmacy (NABP) oversee these operations (see Figure 2). NABP runs the VIPPS (Verified Internet Pharmacy Practice Sites) programme, which certifies pharmacies that meet high standards for safety, legality and privacy. Another useful tool is *PharmacyChecker*, an independent platform that verifies international online pharmacies and helps consumers compare medication prices, making it easier to find safe and affordable options.

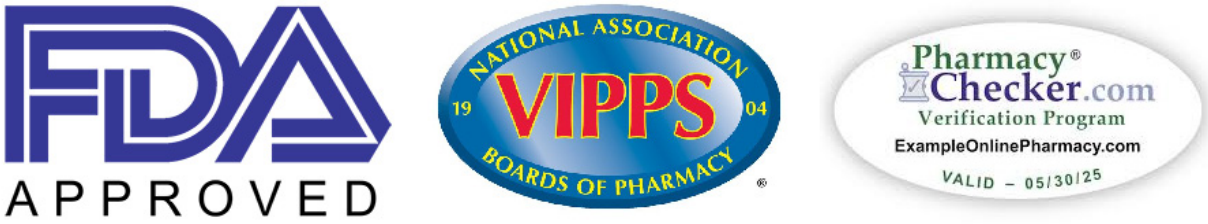

Figure 2: FDA and NABP certification badges, along with the PharmacyChecker verification logo, indicating the legitimacy of an online pharmacy.

Canadian online pharmacies are especially popular among US consumers due to significantly lower drug prices, thanks to Canada's price regulation policies. Although importing medications from Canada is technically not legal under US law, authorities often tolerate it when done for personal use. Trust in Canada's healthcare system also contributes to this trend. Reputable Canadian pharmacies are usually members of the Canadian International Pharmacy Association (CIPA) or the International Pharmacy Association of British Columbia (IPABC), as illustrated in Figure 3. Both organizations certify pharmacies that follow strict safety, ethical, and operational standards. Certified sites often display seals from these associations, which users can verify online.

Figure 3: CIPA and IPABC certification logos indicating membership in recognized pharmaceutical accreditation bodies.

In addition to pharmacy-specific certifications, some online pharmacies also seek Better Business Bureau (BBB) accreditation. The BBB evaluates businesses based on transparency, customer service, and complaint resolution. A BBB-accredited pharmacy (see Figure 4) demonstrates a commitment to ethical business practices, which can provide added peace of mind for consumers – especially when combined with certifications like VIPPS, CIPA, or IPABC.

Figure 4: Better Business Bureau (BBB) accreditation logo indicating trustworthiness and business reliability.

However, consumers should be cautious: some websites may display badges or logos of well-known organizations without actual verification. These images can be misleading and are sometimes used to create a false sense of legitimacy. Always verify such symbols by checking the certifying body's official website.

In contrast, fake online pharmacies show several red flags that should alert consumers. One of the most well-known indicators is the sale of prescription medications without requiring a valid prescription, which legitimate pharmacies never allow [5, 6]. These rogue sites often announce unrealistically low prices and discounts, especially on brand-name drugs, to lure unsuspecting buyers. Unlicensed or unverifiable websites that lack registration with a national authority are also highly suspicious. Additionally, overly positive or generic customer reviews – or the complete absence of credible user feedback – can signal a scam.

However, a more reliable indicator of legitimacy is the presence and quality of reviews on independent platforms like *TrustPilot*. Many fake pharmacies either have numerous negative reviews and scam warnings on *TrustPilot*, or they are not listed there at all. In contrast, legitimate pharmacies usually have a majority of positive reviews, though occasionally some negative ones appear, reflecting a realistic customer experience.

Fake pharmacies frequently offer antibiotics, controlled substances, and other prescription drugs. Common targets include medications for erectile dysfunction (ED), weight loss, and hair loss.

To appear legitimate, fraudulent websites often mimic the look and feel of real e-commerce platforms. They feature shopping carts, multiple payment options, online support, phone contact, FAQs, and even multilingual interfaces. To enhance their appearance of legitimacy, fraudulent websites often display logos of anti-virus companies or mimic certification seals from recognized regulatory authorities despite lacking any actual affiliation or approval. However, during the payment process, users are often redirected to a third-party payment gateway fully controlled by the attackers, putting their personal and financial information at serious risk.

These websites typically lack the mandatory regulatory information mentioned above and exhibit numerous fraud indicators instead.

METHODOLOGY

We utilized a multi-phase approach involving data collection, threat hunting, infrastructure mapping, and telemetry analysis to uncover the underlying infrastructure and classify suspicious online pharmacy websites under a single threat actor.

The first step involved static analysis of suspicious pharmacy websites. This included analysing the source code and on-page content such as listed phone numbers, payment methods, product offerings, and supported languages. These attributes were used to extract IoCs and behavioural patterns.

We then clustered the identified websites based on visual similarity, HTML structure, shared JavaScript components, recurring phone numbers, and identical or similar fake payment gateways. This clustering helped us identify groups of websites probably operated by the same entity.

The second phase focused on dynamic behaviour – specifically, how these websites interact with external servers, how live chat systems operated, and how payment gateways collected sensitive user information. Interactions revealed deeper connections between seemingly unrelated domains.

An additional and particularly effective hunting technique involved analysing DNS records of both fake pharmacy domains and associated payment gateways. Reverse IP lookups helped identify other active domains hosted on the same infrastructure, including less prevalent but still operational sites. This method proved especially useful for discovering newly registered domains tied to known payment gateways, enabling early detection of emerging fake pharmacy sites.

All collected intelligence was used to demonstrate that the identified fake pharmacy websites were not isolated scams, but part of a coordinated operation directed by a single threat actor. We were able to map the broader ecosystem of this cybercriminal network by linking clusters of websites through shared infrastructure and behavioural traits, including the infection vectors used to lure victims to these platforms. Finally, we evaluated this threat's geographic distribution and impact using our telemetry data, gaining insights into its scale and reach across different countries.

SCAMMERS' OPERATION

Reconnaissance

Cybercriminals behind fake online pharmacies begin their operations with detailed reconnaissance. They monitor forums, social media platforms, and online communities to identify high-demand medications. These drugs are typically prescription-only or temporarily unavailable due to supply chain issues.

The most frequently targeted categories include erectile dysfunction medications such as *Viagra* and *Cialis*, followed by antibiotics like amoxicillin and doxycycline. A key psychological factor pushing victims to seek these drugs online is the fear or shame of discussing sensitive health issues with a doctor.

Fake pharmacy shops exploit this exposure by offering not only erectile dysfunction and hair loss treatments but also medications for sexually transmitted infections, including HIV (e.g. lopinavir), hepatitis C (e.g. ribavirin), and syphilis (e.g. amoxicillin). Additionally, they often list anti-viral drugs that become highly sought-after during flu seasons.

A notable example was the demand for ivermectin during the COVID-19 pandemic. Despite being proven ineffective against the virus [7, 8], misinformation and fear led many to seek it online. Looking ahead, we predict similar exploitation of shortages, such as the current absence of anti-depressants like quetiapine [9], which may pressure individuals into risky online purchases.

Weaponization and fake shop link delivery

Attackers move to the weaponization phase when the reconnaissance is complete. The attackers register relevant domains, create a fake online pharmacy website, and set up fraudulent payment gateways. The next step is distributing links to these counterfeit shops as widely and effectively as possible.

We categorize the delivery methods into active and passive approaches.

Active delivery methods

- **Spam campaigns**: Attackers send promotional emails (see Figure 5) resembling flyers with exclusive offers. These emails often contain direct links to a fake pharmacy.

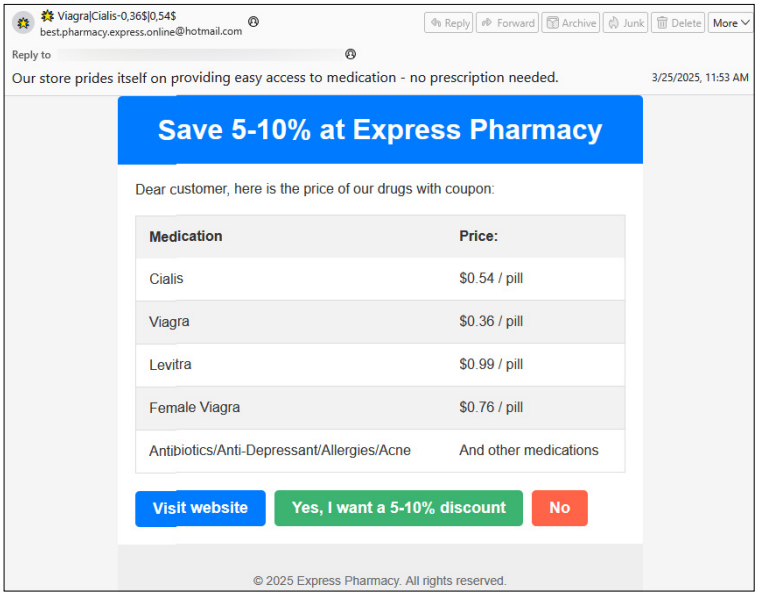

Figure 5: Screenshot of a spam email containing a deceptive link redirecting to a fake online pharmacy website.

- **Online advertisements**: Banner ads are placed on websites with explicit or adult content (see Figure 6), where erectile dysfunction drugs are commonly promoted. However, similar ads have also been observed on mainstream platforms like *Facebook* and *YouTube*, where attackers manipulate legitimate ad services that do not verify the content or do so with delays.

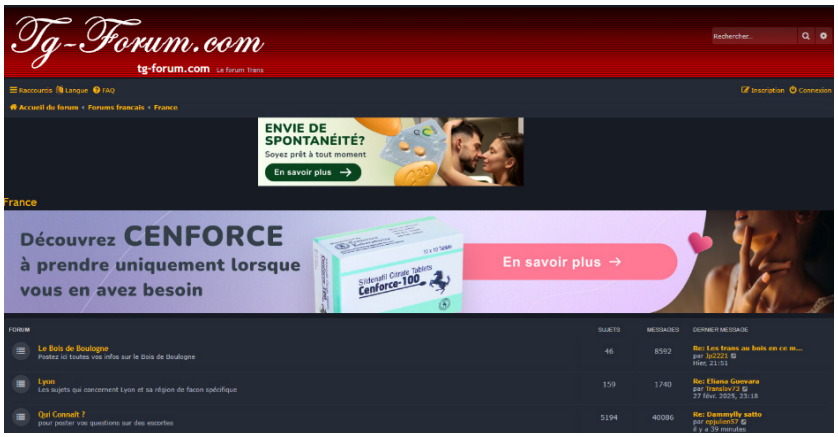

Figure 6: Banner advertisement displayed on a website with explicit or adult content, linking to a fake online pharmacy.

- **Digital flyers**: Platforms like Telegra.ph are used to publish promotional content anonymously with embedded links to fake pharmacies (see Figure 7). Similar flyers are also found on compromised websites, as discussed in the next section.

Figure 7: Examples of promotional flyers published on Telegra.ph, advertising a fake online pharmacy and linking directly to the fraudulent website.

- **Fake review sites**: More than 10 websites (e.g. PharmReviews.net) have been spotted online offering legitimate reviews of online pharmacies. They include reviews of real health-related websites, but the lack of transparency undermines credibility – no verifiable ownership, vague contact details, and inactive social media links. Although some fake pharmacies get negative reviews and are not recommended, the 'Top Rated' section is the most suspicious, including only known fake pharmacies, misleading users into trusting fraudulent pharmacy sites.
- **Fake health blogs**: These blogs, often hosted on domains like '.su', publish AI-generated wellness-related articles. Web visitors encounter banner ads between the articles or are redirected to fake pharmacies on clicking (see Figure 8). These blogs are multi-lingual and optimized for search engines, increasing the likelihood of attracting victims searching for health advice.

Figure 8: Example of a fake health blog where users encounter banner ads redirecting to a fake pharmacy website upon clicking.

Passive delivery methods

Passive methods depend on the victim's actions. Users actively searching for prescription medications may experience fake pharmacies through search engines. To make this possible, attackers manipulate search engine indexing and exploit vulnerabilities in legitimate websites to boost the visibility of their fraudulent content.

While active methods often involve legally questionable tactics like spam and fake reviews, passive methods typically require unauthorized access to compromised web servers – making them more technically sophisticated and complex to detect.

Index manipulation

One of the most effective techniques cybercriminals use to increase the visibility of fake pharmacy websites is index manipulation – the abuse and compromise of legitimate (especially *WordPress*-powered) websites with strong reputations and high search engine rankings.

Attackers inject malicious content into these trusted websites to alter their behaviour and redirect unsuspecting users to fraudulent online pharmacies. We observed three basic types of injection.

Conditional redirect injection

This method triggers a redirect to a fake pharmacy only when the victim arrives via a search engine like *Google* or *Yahoo*. For example, a search for 'cialis online without prescription' may return several top results that appear legitimate but which redirect to fake shops (see Figure 9). These redirects are often embedded in pages like 'contact-us' or 'about', where users would not expect to find pharmaceutical content. Consequently, search engines index these pages using content scraped from the fake pharmacy, which may confuse the victim.

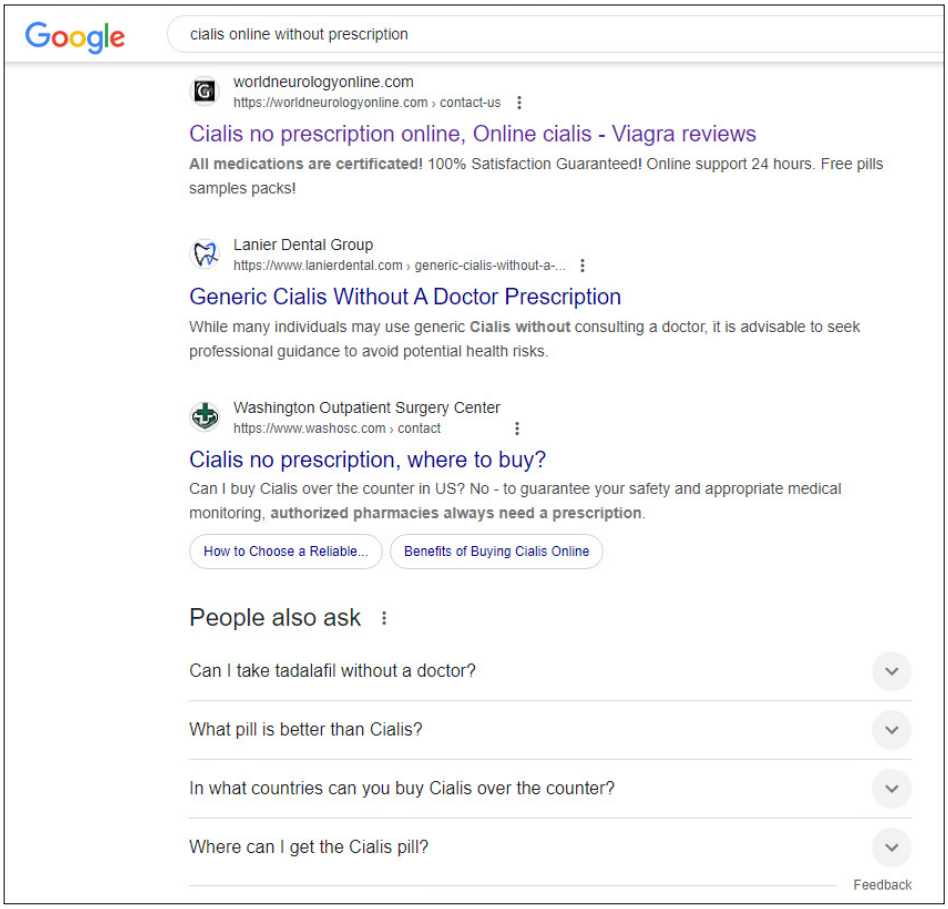

Figure 9: Search engine results showing conditional redirect injection, where users are redirected to a fake pharmacy website only when arriving via a search engine query.

Content injection with redirect

Here, attackers inject an entire page containing information about a specific drug, including links to the fake pharmacy (see Figure 10). If accessed through a search engine, the user is automatically redirected. However, if the page is visited directly, the injected content is displayed on the compromised domain, giving the illusion of legitimacy, especially if the domain of a medical facility is attacked.

In some cases, attackers inject a fully functional fake pharmacy page with active links and a design identical to that of the real shop. When the user clicks anywhere, he is seamlessly redirected to the fake pharmacy domain, making the transition appear legitimate.

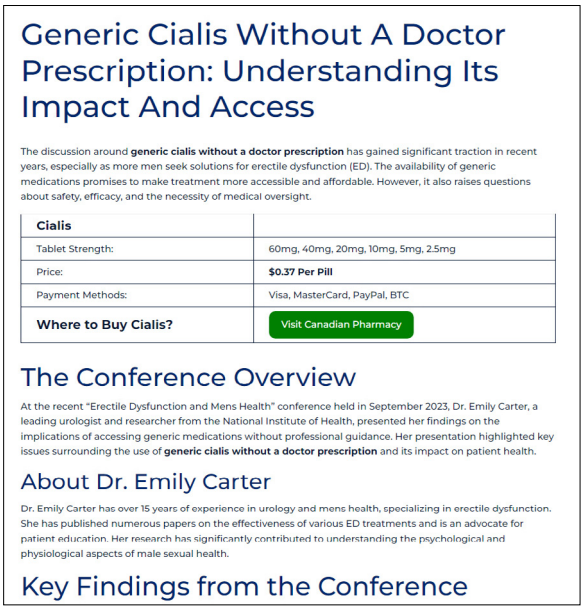

Figure 10: Example of content injection with redirect, where an entire page about a specific drug is injected into a compromised website, including links that lead to a fake online pharmacy.

Brand impersonation

Another manipulation tactic involves brand impersonation. Attackers create fake pharmacy websites using real pharmacies' names, addresses and branding. They register domains using typosquatting techniques – slightly altered versions of legitimate domain names. These fake sites often index highly in search results due to SEO manipulation and content similarity (see Figure 11). Additionally, new ones quickly appear under different TLDs when such domains are taken down, continuing the cycle. To maintain this strategy, attackers actively monitor pharmacies across various countries, looking for brands that can be abused to attract potential victims.

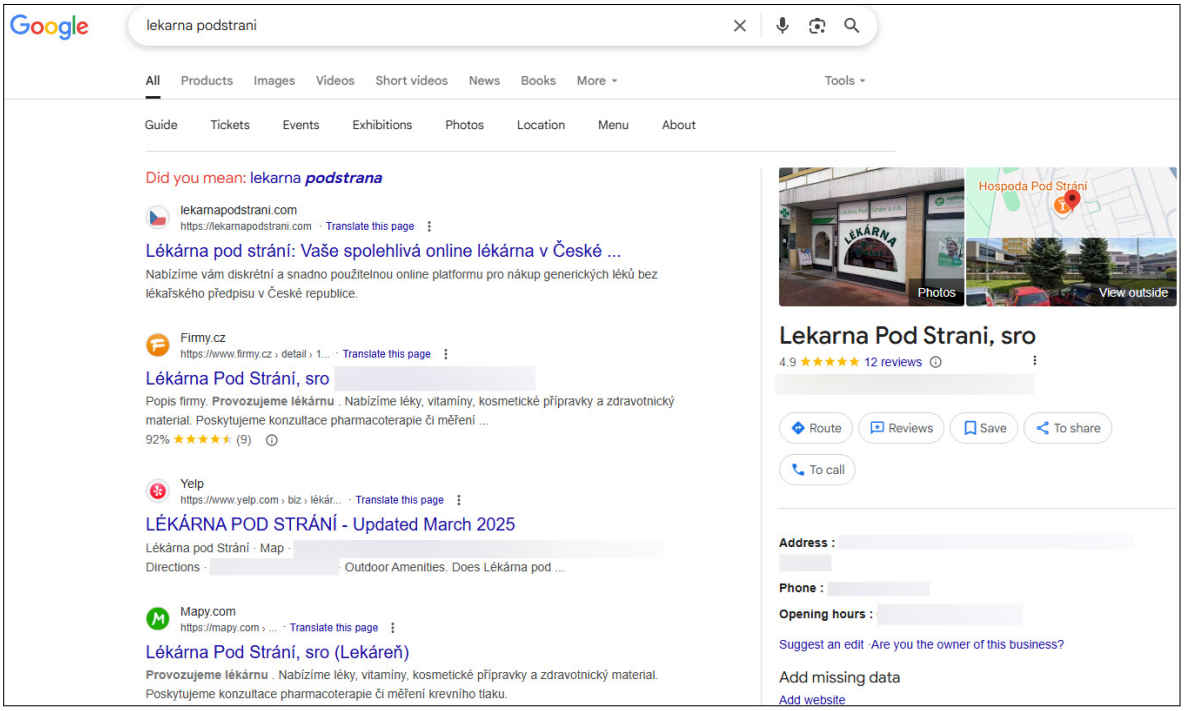

Figure 11: Brand impersonation example – a fake pharmacy site mimicking a real one using typosquatting and SEO to appear in search results.

Another technique attackers use is to register a domain name that closely mimic a legitimate pharmacy (see Figure 12) – either by using a common typo or by changing the top-level domain (TLD) – and deploy a fake shop on it, which can then appear among the top search engine results due to deceptive indexing tactics.

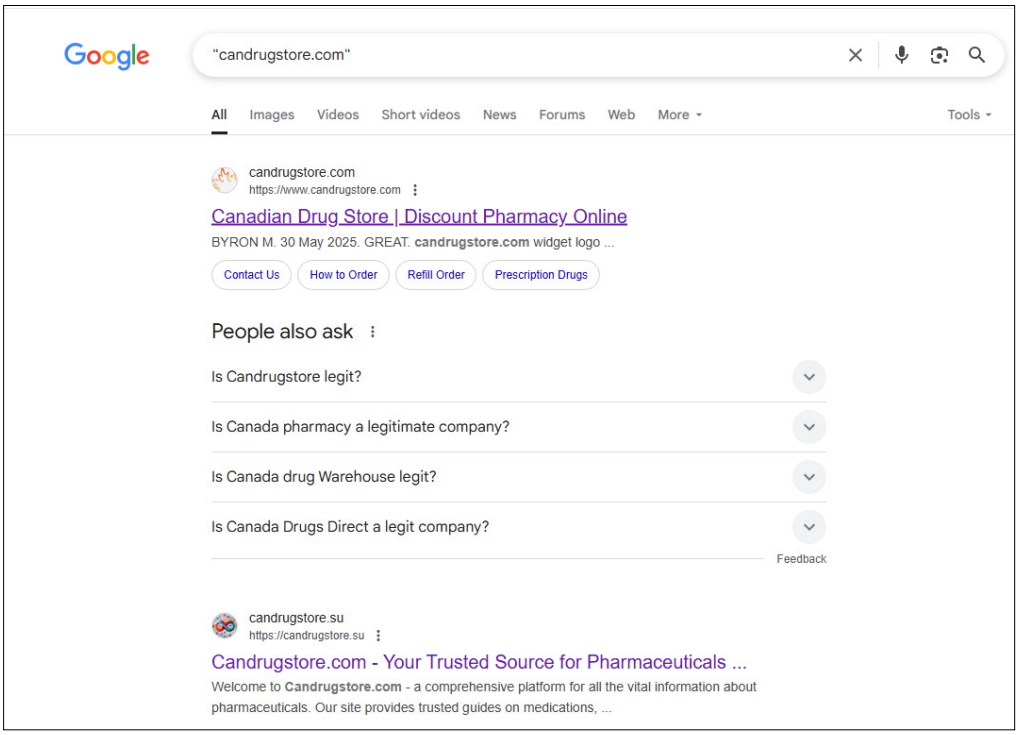

Figure 12: Brand impersonation using a legitimate pharmacy's name with only the TLD changed, leading to a fake shop in search results.

The consequence of these manipulation techniques is that fake pharmacies can appear among the top 10 search results, which significantly increases the likelihood of user exposure and fraud.

A side effect of index manipulation is the potential poising of AI-powered chatbots that can recommend these fake sites unknowingly. Since chatbots often depend on indexed web content, they may include links to fraudulent pharmacies in their responses. For example, a prompt in Greek asking where to buy Cialis online returned a chatbot response with a link to a known fake pharmacy (see Figure 13) –further illustrating the risks of manipulated indexing.

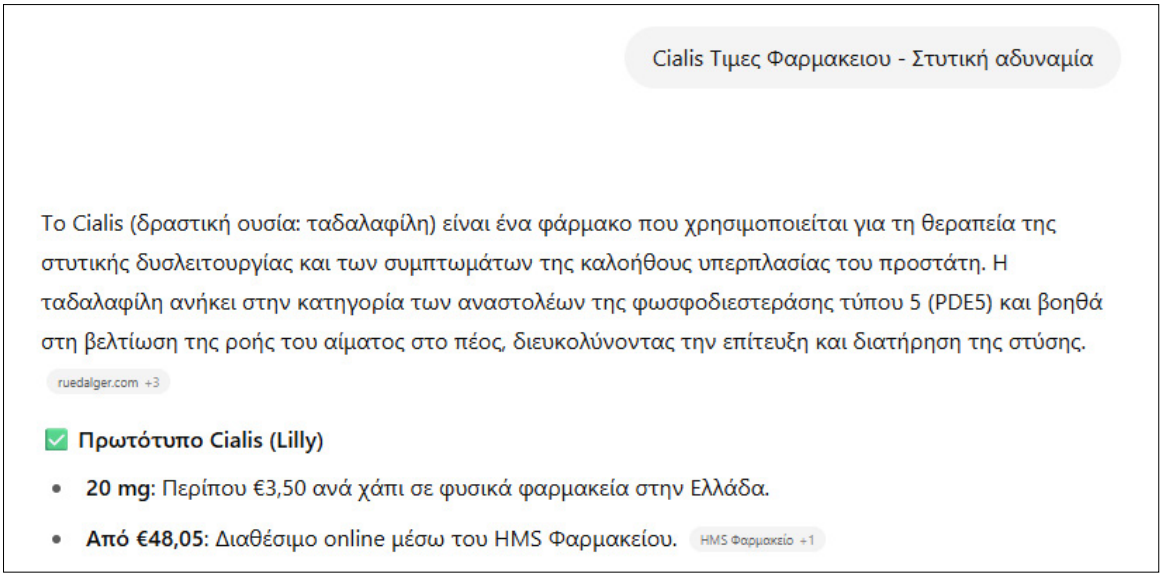

Figure 13: Chatbot response to a Greek-language query about buying Cialis online, returning a link to a known fake pharmacy website.

Exploitation

Once index manipulation or fake shop link delivery is successful, the victim lands on a fraudulent pharmacy website. If the visitor fails to recognize the warning signs – such as lack of licensing, suspiciously low prices, or missing contact details – they may proceed through a seemingly typical shopping workflow, ultimately leading to exploitation.

The purchasing process mimics legitimate e-commerce platforms: the user adds items to a cart and proceeds to checkout. However, the payment gateway (see Figure 14) is typically hosted in a separate domain that the attackers fully control, so there is no secure or legitimate payment processor.

To complete the purchase, the victim is prompted to enter private contact details and payment information, usually a credit card or cryptocurrency wallet which offers a 10% discount. Since the payment gateway is under the attacker's control, all submitted data is directly transmitted to the threat actor.

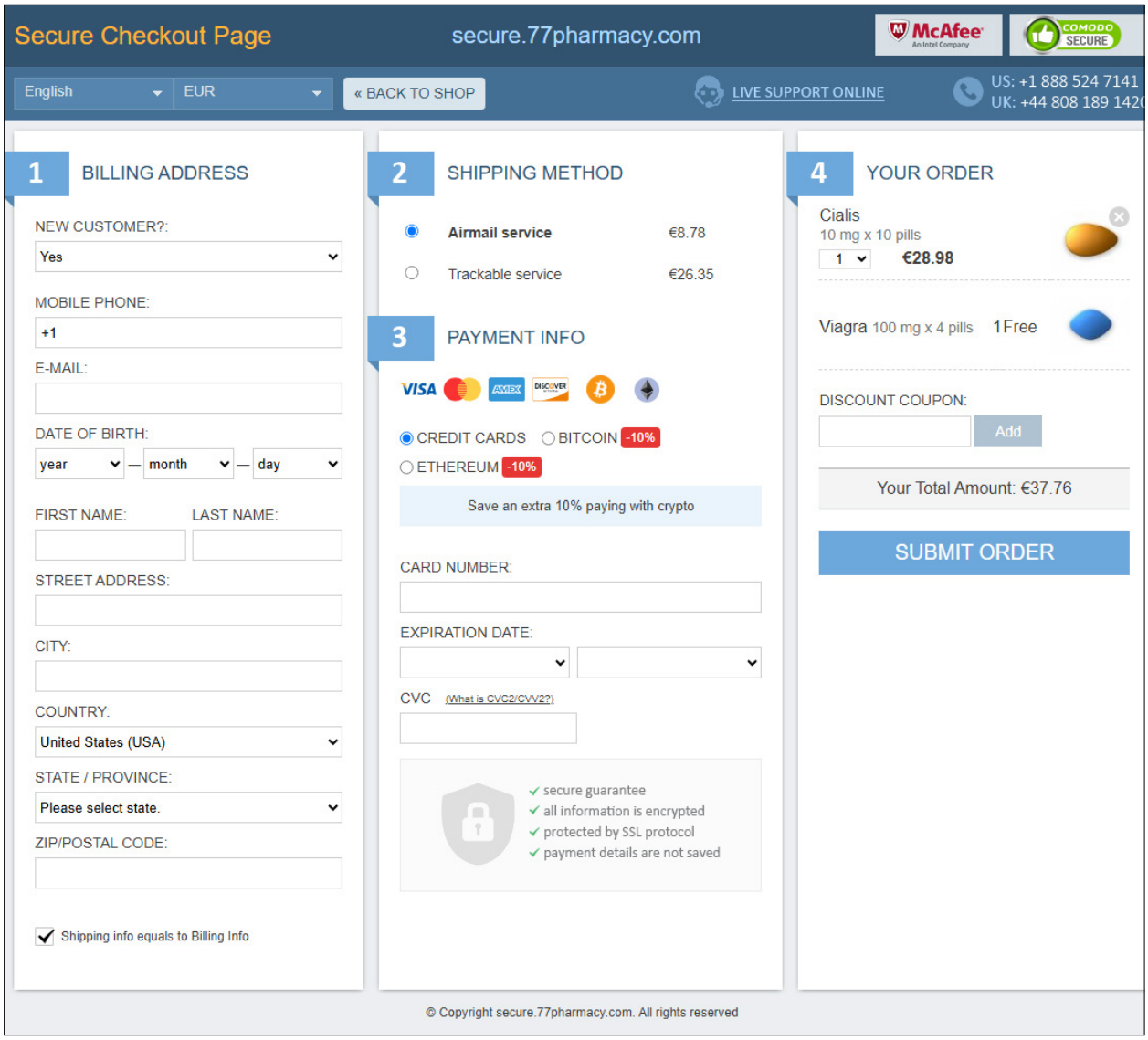

Figure 14: One of the most frequently used payment gateways on fake pharmacy websites, offering a discount when Bitcoin is selected as the payment method.

Fake pharmacy websites often include live chat features or phone numbers for customer support. These communication channels are functional, answering questions about products and the ordering process to build trust.

During our research, we simulated the ordering process using test payment cards. The order was confirmed, and we received a message that if the card was blocked, the user should contact their bank to reactivate it to complete the purchase. This is a clear example of social engineering designed to manipulate the victim into taking further action that benefits the attacker.

Actions on objectives

As we did not complete any real purchases during this research, we cannot confirm whether the attackers delivered any products – be they authentic, counterfeit, or placebo. However, what is certain is that the attacker collects and controls all the payment and contact information entered by the victim.

This data can be used for unauthorized financial transactions or sold on dark web marketplaces. In some cases, the fake payment gateways also include a health questionnaire, requesting sensitive information such as the victim's date of birth

and medical anamnesis. The additional data collection is presented under the camouflage of a medical review to ensure the medication is safe for the user, but in reality, it is another method of collecting exploitable personal data.

The combination of financial, personal and medical information makes victims highly vulnerable to identity theft, financial fraud, and further targeted attacks.

NETWORK ARCHITECTURE

We can outline the network architecture (see Figure 15) supporting illegal online pharmacies' ecosystems based on the IoCs and artifacts collected throughout our research.

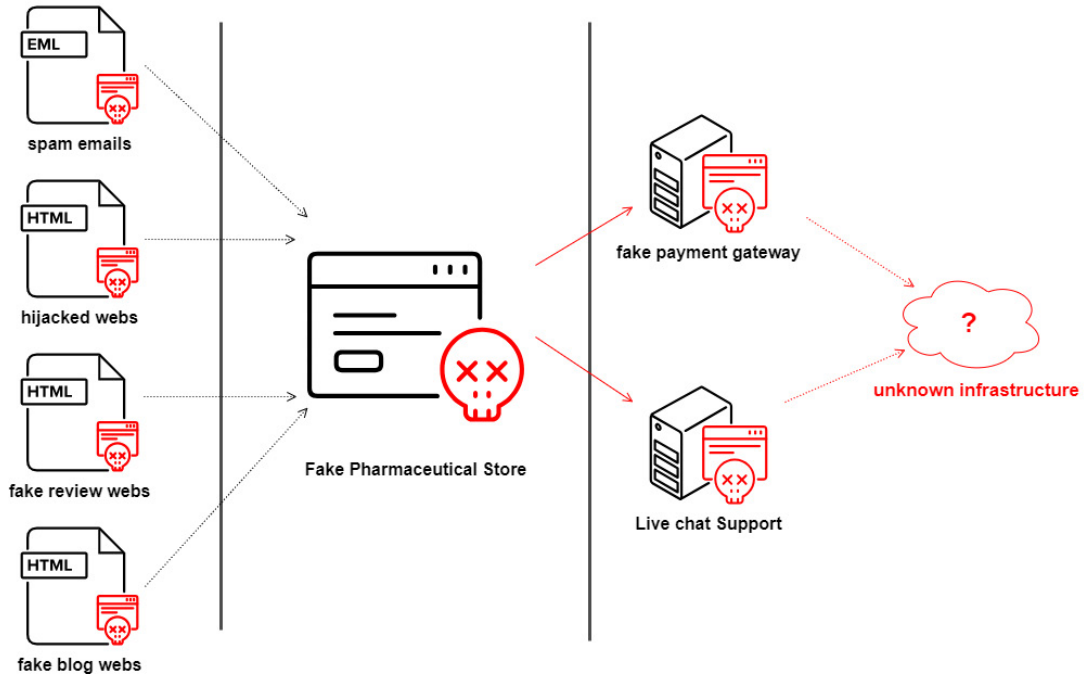

Figure 15: Network architecture diagram of the analysed ecosystem.

At the top level, attackers operate a redirection layer to navigate victims from manipulated search results or malicious advertisements to fake pharmacy websites. These sites then communicate with backend infrastructure, including payment gateways and live chat systems, which collect sensitive data from victims under the guise of customer service or transaction processing.

Key components of the infrastructure

- **Payment gateways**:
  We identified approximately 60 unique domains used for fraudulent payment processing that utilize around 35 templates. Depending on the fake pharmacy branding and target audience, the gateway can be designed to customize itself.

  While the majority of these fraudulent websites redirect users to external domains for payment processing, a smaller subset embeds the checkout process directly within their own domain. These embedded gateways, though less prevalent, maintain a consistent visual style and interface, potentially increasing user trust by mimicking legitimate e-commerce experiences.

- **Live chat systems**:
  Two types of live chat implementations were observed with real people behind them (see Appendix):

  - An open-source solution based on *LiveZilla*.

  - A custom-built live chat platform, likely developed in-house by the attackers.

- **Fake pharmacy domains**:
  Our telemetry revealed at least 5,000 domains hosting fake pharmacy stores. Additionally, websites support adapting to appropriate language and currency, targeting users across different continents.

- **Phone numbers**:
  Dozens of unique phone numbers were collected from fraudulent websites, suggesting the existence of a centralized, call-centre-like infrastructure used to manage victim interactions.

- **Domain growth trends**:
  Analysis of domain registration dates shows an exponential increase starting around 2020 (see Figure 16), coinciding with the COVID-19 pandemic. Much of this growth is likely due not only to new sites, but also to frequent domain rotation – often triggered by blacklisting, takedowns, or reputational damage. This tactic helps to evade detection and maintain continuity.

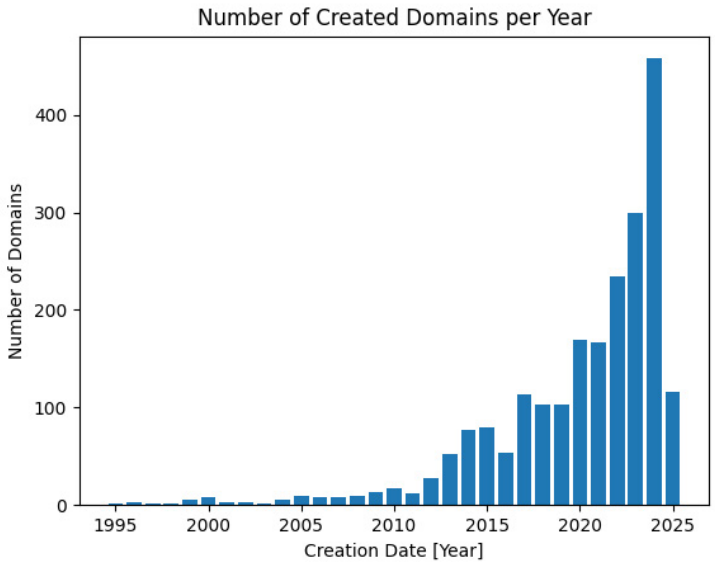

Figure 16: Distribution of domain creation dates over time, illustrating registration trends within the fake pharmacy ecosystem.

- **SSL and hosting infrastructure**:
  Most domains use SSL certificates from *Let's Encrypt*, *Sectigo*, or *Google Trust Services*, with no certificate reuse across sites. Hosting is globally distributed, involving both major providers like *OVHcloud* and *Cloudflare*, and lesser-known ones such as *Sharktech.net*, *IPVolume.net* and *Serveroffer.lt*.

  Several obscure providers – including Phaselayer.com, Pro-spero.ru, Proton66.ru and Pindc.ru – have been linked to scam activity in public reports. Some lack even a functioning website, suggesting weak or non-existent abuse handling. This fragmented setup likely reflects an intentional strategy to avoid centralized detection and takedown.
- **Domain discovery through reverse IP lookups**:
  Reverse IP lookups proved to be a valuable technique for expanding the visibility of the infrastructure. In cases where *Cloudflare* was not used, a single IP address often hosted a large number of domains belonging to the same fake pharmacy cluster or payment gateway infrastructure. Overall, DNS-based analysis served as a powerful tool for uncovering less visible but still active domains and increasing the coverage of threat detection.

This layered and distributed infrastructure allows attackers to maintain stability, avoid takedowns, and continuously adapt their tactics. The system's modularity – where fake shops, payment gateways and communication channels are loosely connected – enables rapid redeployment and rebranding when individual components are exposed or blocked.

ONE ACTOR, MANY DOMAINS

Through continuous monitoring of the fake pharmacy ecosystem – including storefronts, payment gateways, live chat systems, templates, phone numbers, fake review sites, and promotional blogs – we were able to cluster individual shops based on shared infrastructure and behavioural indicators.

The primary objective of this research was to connect these clusters using multiple link rules to determine whether they could be attributed to a single threat actor (STA).

Linkage rules and cluster correlation

- **Live chat and payment gateways systems**:
  One of the most reliable indicators of fake pharmacy websites was using specific live chat platforms, which we observed exclusively on these fraudulent sites. Each fake shop that used one of these live chat tools belonged to a distinct cluster, and each of these clusters was linked to a particular group of payment gateways (see Figure 17). These payment gateways, in turn, formed their cluster, which we could attribute to the STA. As a result, any shop using one of the identified live chat platforms or one of the associated payment gateways is classified as a fake shop operated by

the STA. Additionally, we identified clusters of shops that did not use live chat but were still connected to the same payment gateway cluster. These shops are also attributed to the STA.

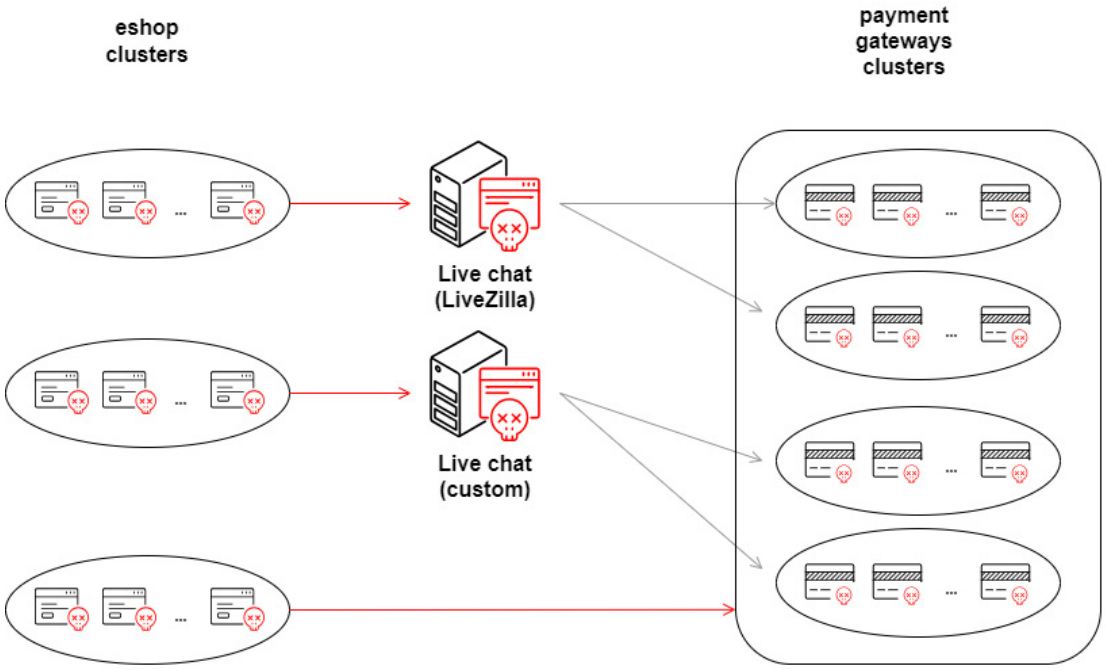

Figure 17: Clustering based on live chats and payment gateways.

- **Phone numbers**:
  Some fake shops do not use live chat and instead display only a phone number – a phone number was present on all but one of the domains analysed. We introduced an additional clustering rule based on phone numbers to account for this (see Figure 18). So, any unknown e-shop that shares one of these phone numbers is attributed to the STA. Consequently, this rule also helps expand the cluster of known payment gateways linked to the STA.

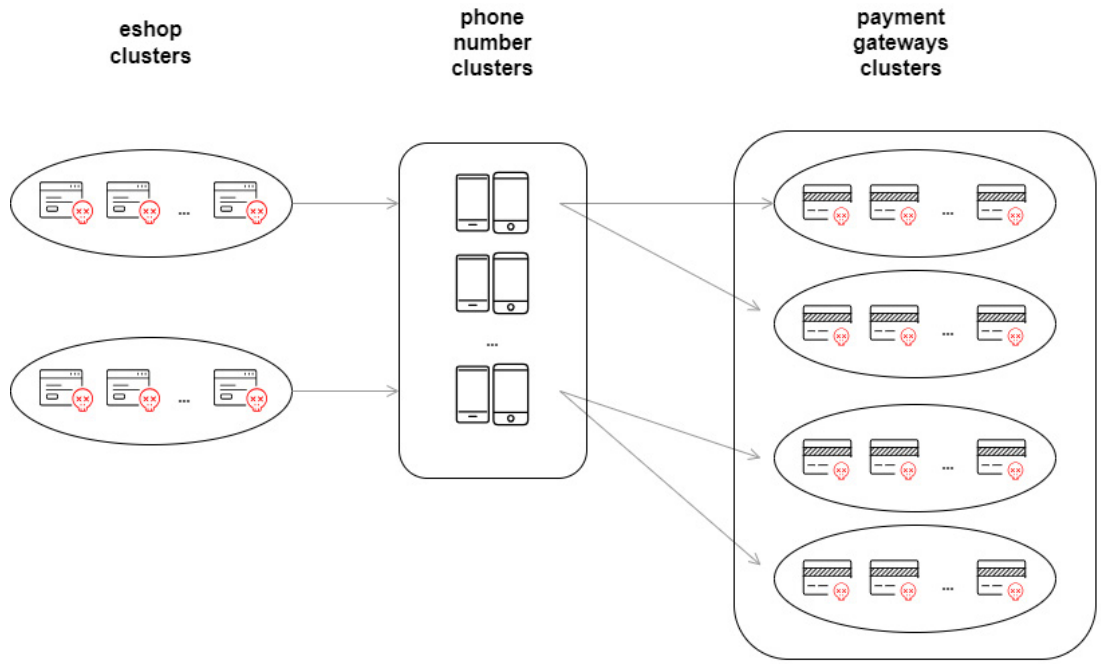

Figure 18: Clustering based on phone numbers.

- **Transitive relationships**:
  These linkage rules enabled us to define relationships between the various network artifacts. We connected seemingly unrelated clusters and artifacts under the STA by applying transitive closure logic. This approach also allows for the future classification of new domains as they appear over time.

- **Temporal correlation**:
  For completeness, some clusters were linked to the STA only over time – for example, when an initially isolated domain later redirected to a known payment gateway.

  Redirect behaviour varied dynamically: the same domain could lead to different pharmacy brands depending on how it was accessed (e.g. via search engine vs. direct input), or the hosted brand changed over time without DNS changes. In some cases, internal redirects transferred users – including cart data – to other shops. These patterns revealed hidden links between clusters of brands, phone numbers, and payment gateways.

Despite diverse branding, the infrastructure points to the single, highly organized threat actor orchestrating a vast network of fake pharmacy websites. Frequent changes observed over short timeframes – often within weeks – suggest high operational activity, likely aimed at evading detection or reflecting ongoing infrastructure restructuring.

DETECTION & DISRUPTION STRATEGIES

Detecting and disrupting fake online pharmacies requires network-based monitoring, static analysis, and continuous feedback loops. Our detection strategy focuses on both behavioural and structural indicators derived from known malicious infrastructure.

Network-based detection

- We monitored communication between suspicious e-shops and known fraudulent payment gateways. Any new connection created between a confirmed fake payment gateway and an unknown shop is automatically classified and clustered as malicious.
- From newly identified fake shops, we extracted additional artifacts – such as phone numbers and live chat systems – which, after verification, are fed back into our detection pipeline to improve future identification.
- Communication between a suspicious website and a known malicious live chat service was also evaluated as a strong indicator of compromise, leading to blocking the associated domain.

Static analysis

- Many large clusters of fake pharmacies consisted of dozens of seemingly unrelated websites, both in terms of source code and visual design. However, they often shared nearly identical, non-malicious JavaScript code used solely for functional purposes.
- Interestingly, while the HTML structure itself varied significantly between sites, the way JavaScript, CSS, and image assets are inlined or embedded follows consistent patterns. This suggests a shared toolkit or deployment process that standardizes how resources are integrated, even if the surrounding HTML is entirely different.
- These recurring patterns enabled effective detection, allowing us to proactively identify new domains using the same infrastructure.

Telemetry

We analysed telemetry data collected from our user base over the past two quarters to evaluate the scale and geographic distribution of the threat.

Key findings

The threat trend is rising, with a noticeable peak during Christmas (see Figure 19), likely due to increased online activity and consumer spending.

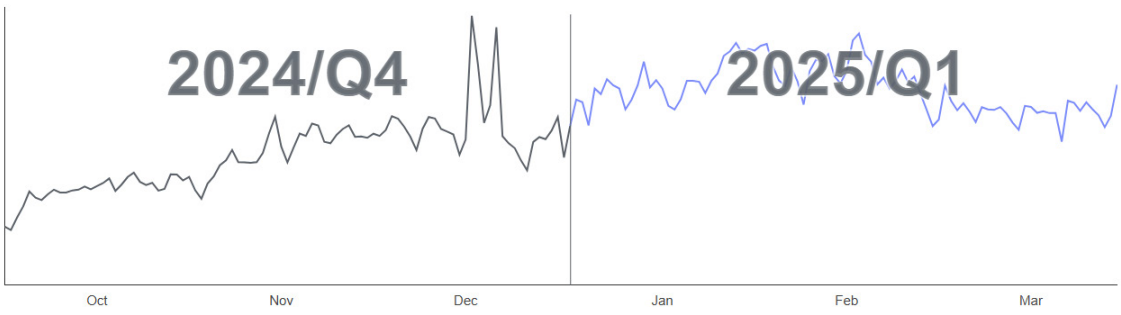

Figure 19: Telemetry data from the past two quarters indicates a rising trend in scale threats, with a pronounced spike observed during the Christmas period.

- We observed approximately 25 language variants of fake pharmacy websites, confirming the campaign's global reach (see Figure 20).
- Based on risk ratios and detection density, attackers appear to be primarily targeting Europe, especially:
  - Southeastern Europe: Greece, Croatia, Hungary
  - Central Europe: Switzerland, Austria
  - Western Europe: France, Spain
- Outside of Europe, significant activity was also detected in Japan, Australia, USA and Canada, indicating that the campaign is not geographically limited.

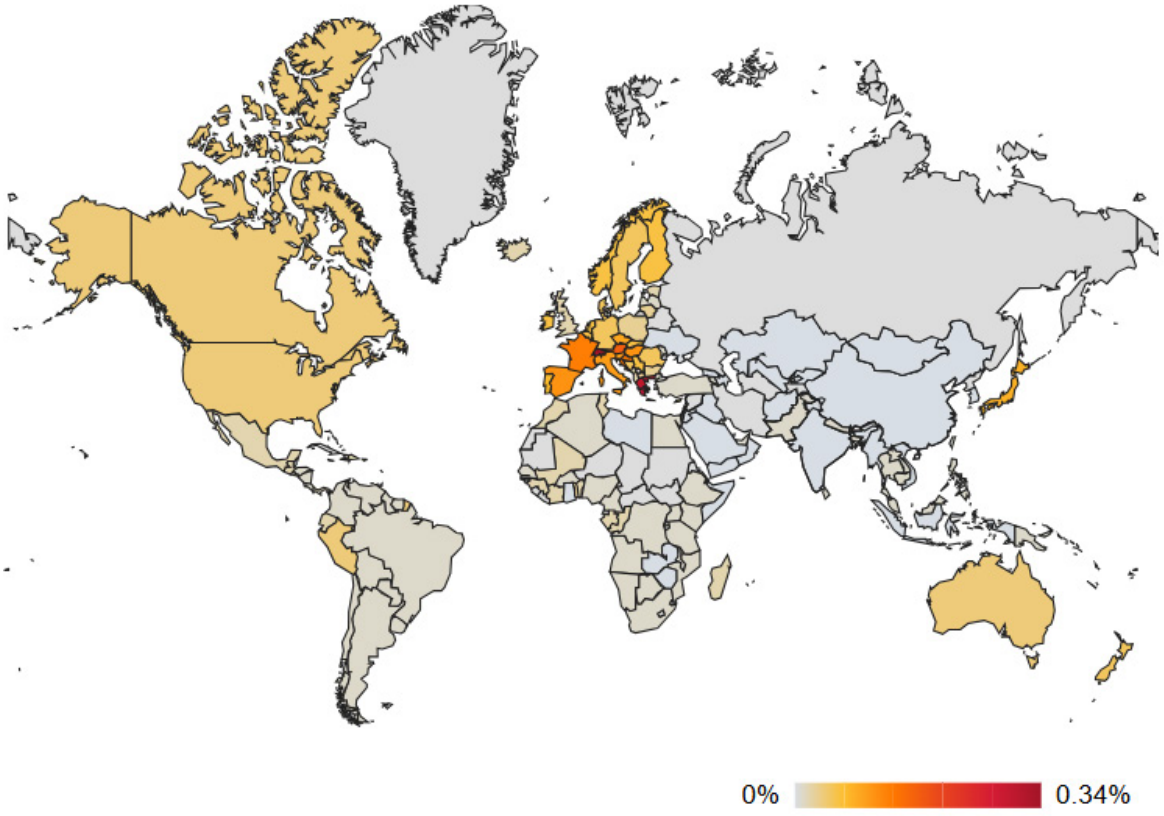

Figure 20: Geographic distribution of the threat based on telemetry data, highlighting regional variations in threat activity across our user base.

This telemetry confirms that the threat actor is operating a highly scalable and multi-lingual infrastructure, capable of adapting to regional markets.

FUTURE WORK

While this research has successfully uncovered a large-scale, coordinated infrastructure behind illegal online pharmacies, several areas remain open for further exploration and development.

Building on the current detection system and threat hunting capabilities, future efforts will focus on continuous monitoring of the identified threat actor's behaviour and infrastructure evolution. This will allow us to adapt and expand our detection methods as new tactics, techniques and procedures (TTPs) emerge.

Another key area for development is the automation of artifact extraction and collection. Automating this process would significantly accelerate the identification and blocking of malicious domains and infrastructure. In this context, experimenting with AI-based tools for pattern recognition and anomaly detection could further improve efficiency and scalability.

Finally, establishing collaboration with international enforcement bodies such as INTERPOL or national cybersecurity agencies could enable domain takedowns and broader disruption of the threat actor's operations. Such partnerships would strengthen the impact of technical findings and contribute to a more coordinated global response.

CONCLUSION

This research has revealed the infrastructure's alarming scale, complexity, and adaptability behind illegal online pharmacies. What may appear to users as isolated, suspicious websites is an extensive, coordinated cybercriminal operation spanning thousands of domains, dozens of payment gateways, and multi-lingual content targeting victims across the globe.

By combining static and dynamic analysis, infrastructure mapping, and telemetry data, we demonstrated that these fake pharmacy networks are technically sophisticated and socially manipulative – exploiting fear, urgency, and misinformation to lure victims. Our findings strongly suggest that a single threat actor or a tightly coordinated group orchestrates this ecosystem, leveraging shared infrastructure components such as live chats, phone numbers, and cloned templates.

The consequences of this threat extend beyond financial fraud. Victims are exposed to serious health risks, identity theft, and long-term data exploitation. Moreover, the manipulation of search engine indexing, abuse of legitimate platforms, and serious pharmacy brand impersonation further amplifies the reach and credibility of these fake shops.

Preventing and mitigating this threat requires better education for internet users – raising awareness about what a legitimate online pharmacy looks like, the importance of certification, and how to verify authenticity. Finally, international cooperation with law enforcement authorities is essential to stop these operations at the source.

REFERENCES

[1] Harvard Health Publishing. Don't get duped: Here's how to avoid online pharmacy risks. 1 August 2023. https://www.health.harvard.edu/staying-healthy/dont-get-duped-heres-how-to-avoid-online-pharmacy-risks.

[2] Taylor, P. Viewpoint: Addressing the rise of pharmaceutical fraud. SecuringIndustry.com. https://www.securingindustry.com/pharmaceuticals/viewpoint-addressing-the-rise-of-pharmaceutical-fraud/s40/a1022/.

[3] Centers for Disease Control and Prevention. Potential public health risk among individuals ordering counterfeit prescription medications from online pharmacies. 2 October 2024. https://www.cdc.gov/media/releases/2024/s1002-counterfit-prescription-online-pharmacies.html.

[4] World Health Organization. Substandard and falsified medical products. 2017. https://www.who.int/news-room/fact-sheets/detail/substandard-and-falsified-medical-products.

[5] U.S. Food and Drug Administration. How to buy medicines safely from an online pharmacy. https://www.fda.gov/consumers/consumer-updates/how-buy-medicines-safely-online-pharmacy.

[6] European Medicines Agency. Buying medicines online. https://www.ema.europa.eu/en/human-regulatory-overview/public-health-threats/falsified-medicines-overview/buying-medicines-online.

[7] Caly, L.; Druce, J. D.; Catton, M. G.; Jans, D. A.; Wagstaff, K. M. The FDA-approved drug ivermectin inhibits the replication of SARS-CoV-2 in vitro. Antiviral Research, 178, 104787. 2020. https://doi.org/10.1016/j.antiviral.2020.104787.

[8] U.S. Food and Drug Administration (FDA). Why you should not use ivermectin to treat or prevent COVID-19. 2021. https://www.fda.gov/consumers/consumer-updates/why-you-should-not-use-ivermectin-treat-or-prevent-covid-19.

[9] European Medicines Agency. Quetiapine – supply shortage. 11 March 2025. https://www.ema.europa.eu/en/medicines/human/shortages/quetiapine.

APPENDIX

To evaluate whether fake pharmacy live chats are run by bots or humans, we conducted simple conversational tests. In Figure 21, the analyst interacts with support using:

1. A riddle, which support answers with a human-like shorthand – placing a ')' directly after a word, mimicking a smiley.
2. A personal question about liking the support's name, answered briefly and plainly.
3. A request for a joke, which support declines – which is unusual for a bot aiming to engage users.

The chat also shows inconsistent capitalization, another sign of human input. In Figure 22, a similar exchange ends with support stating the chat is 'provided by real people'. These clues suggest the presence of human operators rather than AI bots.

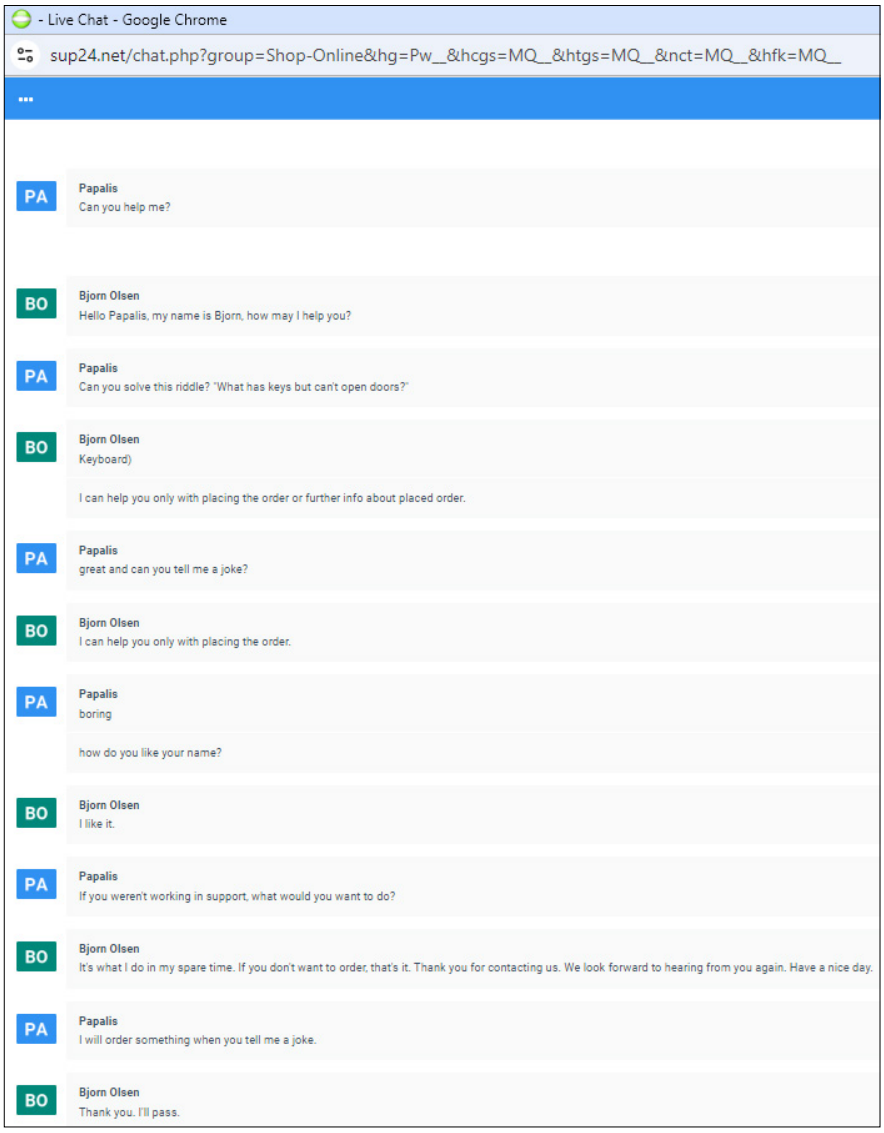

Figure 21: LiveZilla app – communication with live support of a fake pharmacy shop.

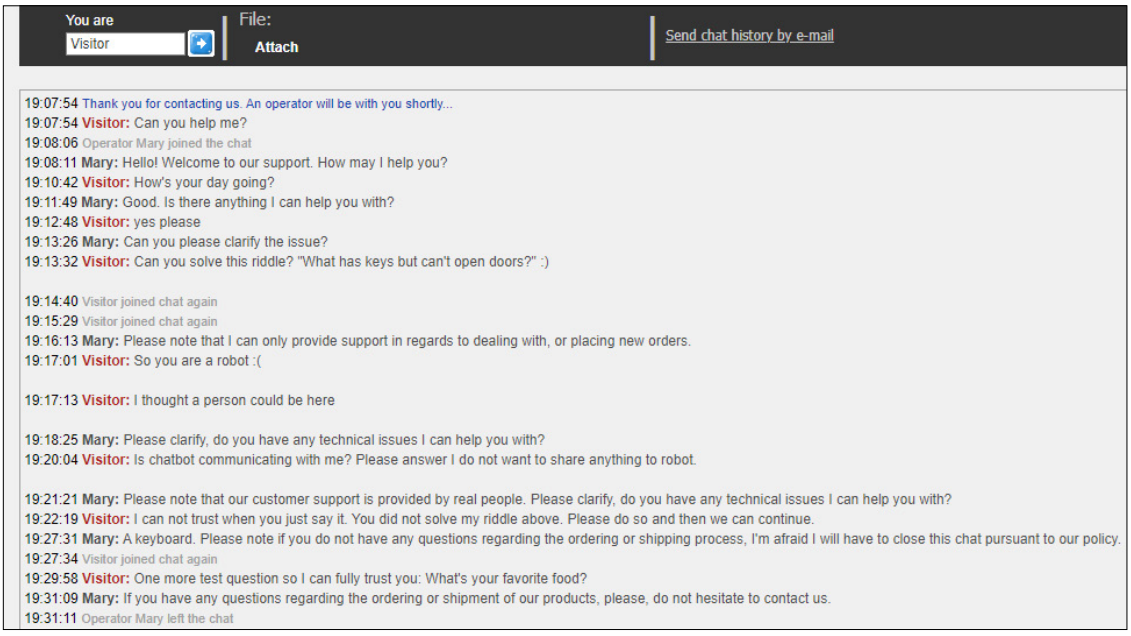

Figure 22: Custom live chat – communication with live support of a fake pharmacy shop.