



The Dark Prescription:

Inside the Infrastructure of Illegal Online Pharmacies

24 Sept. 2025



Hello, Berlin!



- Ľuboš Bever
- Threat Researcher
- Member of Threat Intelligence team
- Focusing on scams
 - Fake e-Shops and PDF threats
- SimRacing in free time



- Jan Rubín
- Threat Research Team Lead
- Leading a specialized team focused on combating data-theft
- Guest lecturer for a reverse engineering course at the CTU in Prague
- Jazz and swing musician

Can You Spot the Scam?

EU Pharmacy

Search by product name

My cart

Viagra, Cialis, Levitra online

Safe and Effective erectile dysfunction drugs

Buy Now

Why Us

- We make millions of people all over the world healthy and happy!
- Fast Global Shipping**
Discreet package
- Friendly support**
Available 24/7
- Online consultation**
Low price online
- High quality products**
Reliable supplier
- Discount for future orders**
Bonus Pills

Bestsellers

Cookies policy
We use our own and third-party cookies to improve the browsing experience and offer content interesting to you. By continuing to browse you accept our cookie policy. For more information contact our specialists.

Accept

Fake Pharmacy

Free delivery on orders over £45 | Use Code W30 for £20 off Wegovy | Mounjaro: Due to high demand, we are only accepting orders for existing patients. Processing time is 7-10 days.

pharmacyonline

Login

Basket

Online Clinic | Shop | Weight Loss | Get In Touch

Your Trusted Online Pharmacy.

Improving the lives of our patients by making high-quality care accessible and convenient

Search Treatments & Products...

Rated 4.73 Based on 5187 Reviews

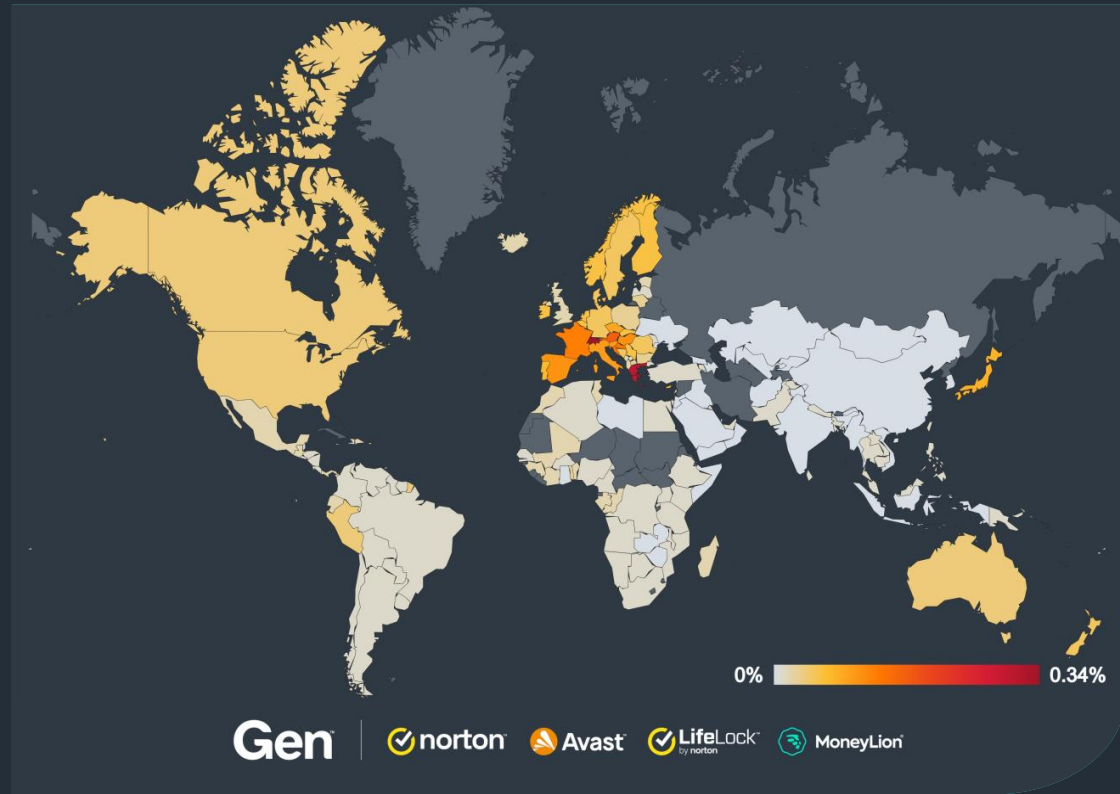
Popular products

- Regaine Foam for Men
- Solpadeine Max - 24 Tablets
- Chloramphenicol Eye Ointment
- Laxido Orange Powder Sugar Free

Legit Pharmacy

Why Fake Pharmacies Are More Than Just a Scam

- Fake e-Shops dataset
 - Huge domain redundancy
- NABP stated [1] [2]:
 - 40,000 unsafe online pharmacies
 - 95% operate illegally
- MediPhantom
 - A global coordinated operation
 - Thousands of domains, cloned storefronts etc.



The Digital Drug Market: Who's Selling, Who's Scamming

Legitimate:

- Strict safety and ethical standards
- Registration with national authorities
 - FDA in U.S.
 - CIPA in Canada
 - BfArM in Germany
- Users can verify online

Fake:

- False sense of legitimacy
- Fake badges and logos
- Cheap prescription pills without prescription
- Overly positive or generic customer reviews
- Fake payment gateways

Popular Categories

ED Packs

Women's Health



Home

About Us

Our Policies

Track

Shop



Copyright © 2025 All rights reserved





How Victims Are Targeted: MediPhantom in Action

Finding the Vulnerable: How Victims Are Selected

- Active monitoring
 - High-demand medications
 - Prescription-only or unavailable
- Erectile dysfunction medications:
 - Viagra and Cialis
- Sexually transmitted infections:
 - HIV (Lopinavir)
 - Syphilis (Amoxicillin)
- Ivermectin during the COVID-19

Bestsellers

Viagra
Active ingredient: Sildenafil
£0.22 for pill
BUY NOW

Cialis
Active ingredient: Tadalafil
£0.55 for pill
BUY NOW

Clomid
Active ingredient: Clomiphene
£0.36 for pill
BUY NOW

Special offer
SALE
Viagra 10 pills x 100mg + Cialis 10 pills x 100mg = BUY NOW £37.39

ED Sample Pack 1
£1.87 for pill
BUY NOW

Brand Viagra
Active ingredient: Sildenafil
£1.43 for pill
BUY NOW

Doxycycline
£0.24 for pill
BUY NOW

Crafting the Trap: From Scam Setup to Link Drop

- Active Delivery Methods
 - Depend on threat actor's action
 - Fake health blogs, fake review platforms, spam campaigns
- Passive Delivery Methods
 - Depend on victim's action
 - Conditional Redirect Injection
 - Content Injection with Redirect
 - Brand impersonation

The screenshot shows the homepage of 'Generic Pharmacy'. The header includes contact information (US Toll Free: +1 888 524 7141, UK: +44 800 189 1420) and navigation icons. A banner at the top lists benefits: 'Free worldwide shipping', 'Bonuses and Discounts', 'Money back Guarantee', 'Save 10% just for using crypto', 'Secure and Reliable', and 'High quality products'. Below the banner is a search bar and a 'Bestsellers' section. The 'Bestsellers' section displays eight products in a grid, each with a discount tag and a 'Buy Now' button. The products are: Viagra (-33%), Cialis (-33%), Kamagra Oral Jelly (-33%), Kamagra (-33%), Levitra (-33%), Viagra Super Active (-33%), Cialis Professional (S...) (-20%), and Lasix (-20%).

Product	Discount	Price per unit	Available strengths	Buy Now
Viagra (Sildenafil Citrate)	-33%	£0.27 per pill	25mg, 50mg, 100mg, 120mg, 130mg, 150mg, 200mg	Yes
Cialis (Tadalafil)	-33%	£0.80 per pill	10mg, 20mg, 40mg, 60mg, 80mg	Yes
Kamagra Oral Jelly (Sildenafil Citrate)	-33%	£1.71 per sachet	100mg	Yes
Kamagra (Sildenafil Citrate)	-33%	£1.06 per pill	100mg	Yes
Levitra (Vardenafil)	-33%	£0.74 per pill	10mg, 20mg, 40mg, 60mg	Yes
Viagra Super Active (Sildenafil Citrate)	-33%	£1.00 per cap	100mg	Yes
Cialis Professional (S...) (Tadalafil)	-20%	£1.57 per pill	20mg, 40mg	Yes
Lasix (Furosemide)	-20%	£0.27 per pill	40mg, 100mg	Yes

Crafting the Trap: From Scam Setup to Link Drop

Active Delivery Methods

ENVIE DE SPONTANÉITÉ?
Soyez prêt à tout moment
[En savoir plus →](#)

Découvrez CENFORCE
à prendre uniquement lorsque vous en avez besoin
[En savoir plus →](#)

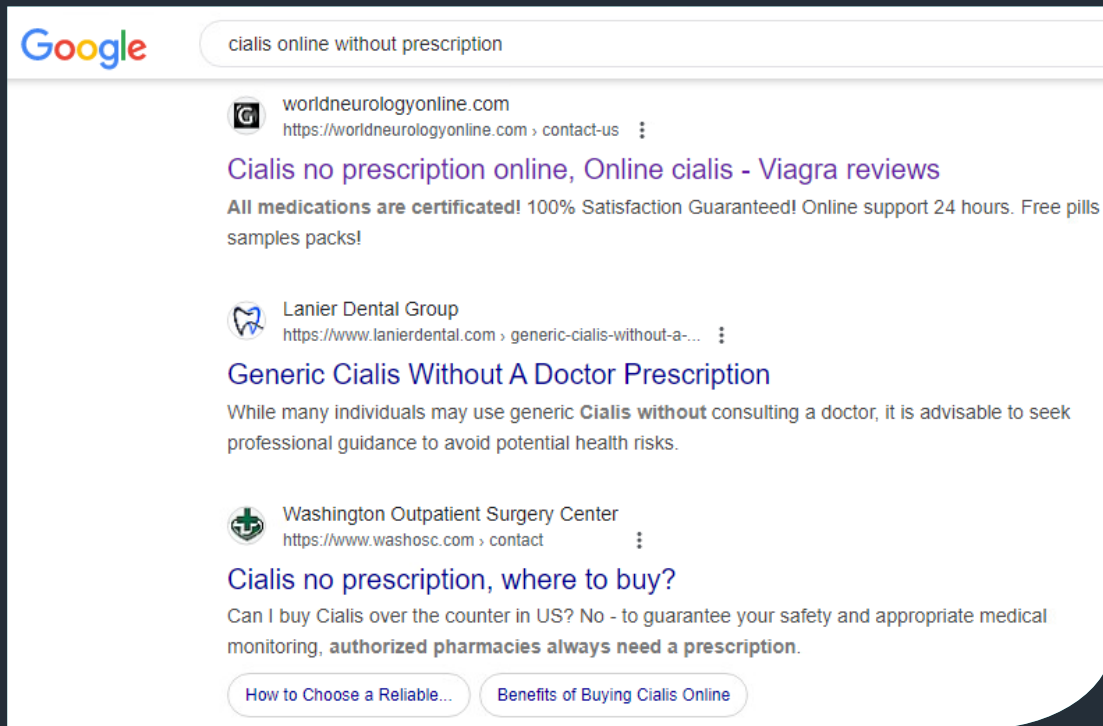
FORUM	SUJETS	MESSAGES	DERNIER MESSAGE
Le Bois de Boulogne Postez ici toutes vos infos sur le Bois de Boulogne	46	8592	Re: Les trans au bois en ce m... par Jo2221 2 Hier, 21:51
Lyon Les sujets qui concernent Lyon et sa région de façon spécifique	159	1740	Re: Eliana Guevara par Translov73 2 27 févr. 2025, 23:18
Qui Connait ? pour poster vos questions sur des escortes	5194	40086	Re: Dammylly satto par epjulien57 2 il y a 39 minutes

Online
Advertisements
Banner ads

Crafting the Trap: From Scam Setup to Link Drop

Passive Delivery Method — SEO Manipulation

- Users actively searching for medications
- Require unauthorized access
- Crawler-bots are confused
- Injection of:
 - Redirection to pharmacy
 - Deceptive content on compromised domain
- Illusion of legitimacy



The screenshot shows a Google search interface with the query "cialis online without prescription". The search results are as follows:

- Result 1:** worldneurologyonline.com
URL: <https://worldneurologyonline.com/contact-us>
Title: **Cialis no prescription online, Online cialis - Viagra reviews**
Text: **All medications are certificated!** 100% Satisfaction Guaranteed! Online support 24 hours. Free pills samples packs!
- Result 2:** Lanier Dental Group
URL: <https://www.lanierdental.com/generic-cialis-without-a-...>
Title: **Generic Cialis Without A Doctor Prescription**
Text: While many individuals may use generic **Cialis without** consulting a doctor, it is advisable to seek professional guidance to avoid potential health risks.
- Result 3:** Washington Outpatient Surgery Center
URL: <https://www.washosc.com/contact>
Title: **Cialis no prescription, where to buy?**
Text: Can I buy Cialis over the counter in US? No - to guarantee your safety and appropriate medical monitoring, **authorized pharmacies always need a prescription.**

At the bottom of the search results, there are two buttons: "How to Choose a Reliable..." and "Benefits of Buying Cialis Online".

Crafting the Trap: From Scam Setup to Link Drop

Passive Delivery Method — SEO Manipulation

Brand impersonation
Mimicking a real
brand

The screenshot shows a Google search for "lekarna podstrani". The search bar contains the text "lekarna podstrani". Below the search bar, there are navigation tabs for "All", "Products", "Images", "Videos", "Short videos", "News", "Books", and "More". There are also "Tools" and "Guide" tabs. The search results include a "Did you mean" suggestion for "lekarna podstrana". The first result is from "lekamapodstrani.com" with the title "Lékárna pod strání: Vaše spolehlivá online lékárna v České ..." and a description: "Nabízíme vám diskretní a snadno použitelnou online platformu pro nákup generických léků bez lékařského předpisu v České republice." The second result is from "Firmy.cz" with the title "Lékárna Pod Strání, sro" and a description: "Popis firmy. Provozujeme lékárnu. Nabízíme léky, vitamíny, kosmetické přípravky a zdravotnický materiál. Poskytujeme konzultace farmacoterapie či měření ... 92% ★★★★★ (9)". The third result is from "Yelp" with the title "LÉKÁRNA POD STRÁNÍ - Updated March 2025" and a description: "Lékárna pod Strání · Map · Directions · Outdoor Amenities: Does Lékárna pod ...". The fourth result is from "Mapy.com" with the title "Lékárna Pod Strání, sro (Lekářeň)" and a description: "Provozujeme lékárnu. Nabízíme léky, vitamíny, kosmetické přípravky a zdravotnický materiál. Poskytujeme konzultace farmacoterapie či měření krevního tlaku." On the right side of the search results, there is a business listing for "Lekarna Pod Strani, sro" with a 4.9 star rating and 12 reviews. The listing includes a photo of the pharmacy building, a "View outside" button, and buttons for "Route", "Reviews", "Save", "To share", and "To call". The listing also shows fields for "Address", "Phone", and "Opening hours", and a link to "Suggest an edit".

Crafting the Trap: From Scam Setup to Link Drop

Passive Delivery Method — SEO Manipulation

Cialis Τιμες Φαρμακειου - Στυτική αδυναμία

Το Cialis (δραστική ουσία: ταδαλαφίλη) είναι ένα φάρμακο που χρησιμοποιείται για τη θεραπεία της στυτικής δυσλειτουργίας και των συμπτωμάτων της καλοήθους υπερπλασίας του προστάτη. Η ταδαλαφίλη ανήκει στην κατηγορία των αναστολέων της φωσφοδιεστεράσης τύπου 5 (PDE5) και βοηθά στη βελτίωση της ροής του αίματος στο πέος, διευκολύνοντας την επίτευξη και διατήρηση της στύσης.

[ruedalger.com](#) +3

✓ Πρωτότυπο Cialis (Lilly)

- **20 mg:** Περίπου €3,50 ανά χάπι σε φυσικά φαρμακεία στην Ελλάδα.
- **Από €48,05:** Διαθέσιμο online μέσω του HMS Φαρμακείου. [HMS Φαρμακείο](#) +1

Poisoned Chatbot

“Cialis Pharmacy Prices – Erectile dysfunction”

The Click That Costs: When the Scam Hits

- Typical shopping workflow
- Not secure payment gateway
 - Often separate domain
 - Attackers fully control
- Solicited sensitive details:
 - Date of birth
 - Medical anamnesis
- Customer support:
 - Live chat & phone numbers

Secure Checkout Page secure.77pharmacy.com

English EUR « BACK TO SHOP LIVE SUPPORT ONLINE US: +1 888 524 7141 UK: +44 808 189 1420

1 BILLING ADDRESS

NEW CUSTOMER?: Yes

MOBILE PHONE: +1

E-MAIL:

DATE OF BIRTH: year month day

FIRST NAME: LAST NAME:

STREET ADDRESS:

CITY:

COUNTRY: United States (USA)

STATE / PROVINCE: Please select state.

ZIP/POSTAL CODE:

Shipping info equals to Billing Info

2 SHIPPING METHOD

Airmail service €8.78

Trackable service €26.35

3 PAYMENT INFO

CREDIT CARDS BITCOIN -10% ETHEREUM -10%

Save an extra 10% paying with crypto

CARD NUMBER:

EXPIRATION DATE:

CVC (What is CVC2/CVV2?)

secure guarantee
all information is encrypted
protected by SSL protocol
payment details are not saved

4 YOUR ORDER

Cialis 10 mg x 10 pills €28.98

Viagra 100 mg x 4 pills 1Free

DISCOUNT COUPON: Add

Your Total Amount: €37.76

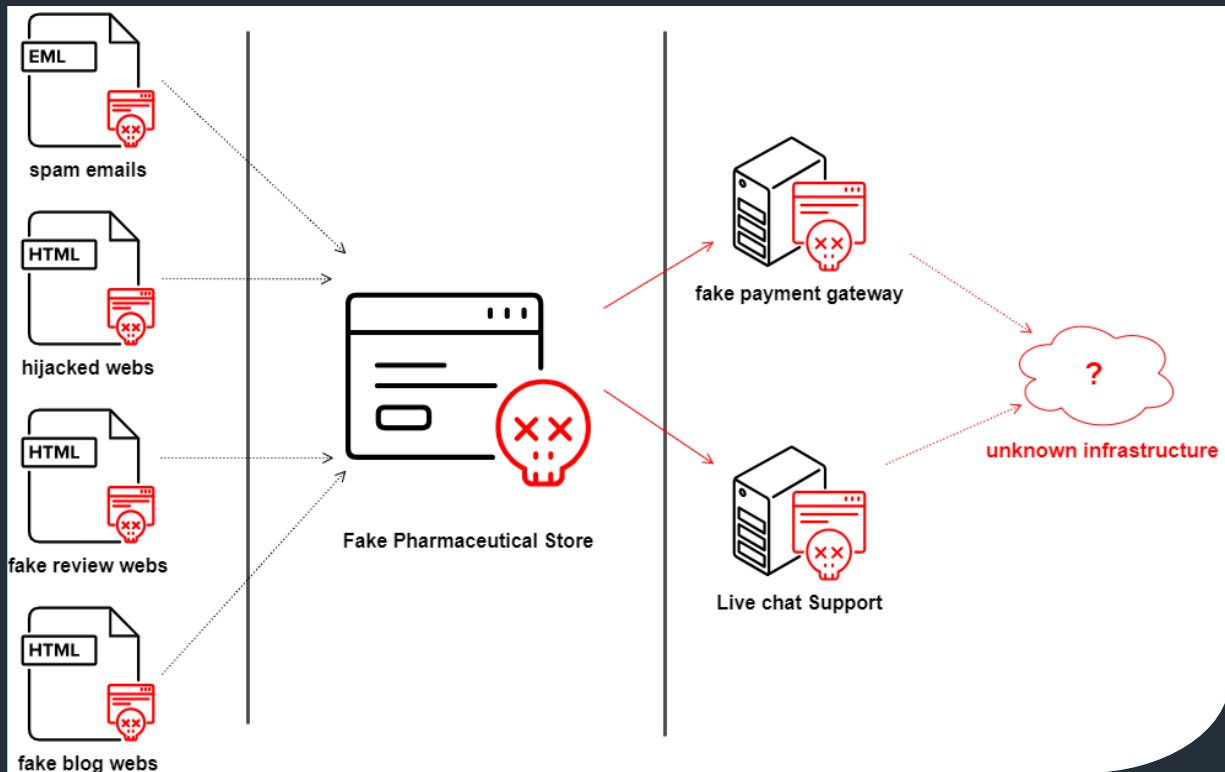
SUBMIT ORDER

© Copyright secure.77pharmacy.com. All rights reserved

The Hidden Infrastructure Behind MediPhantom

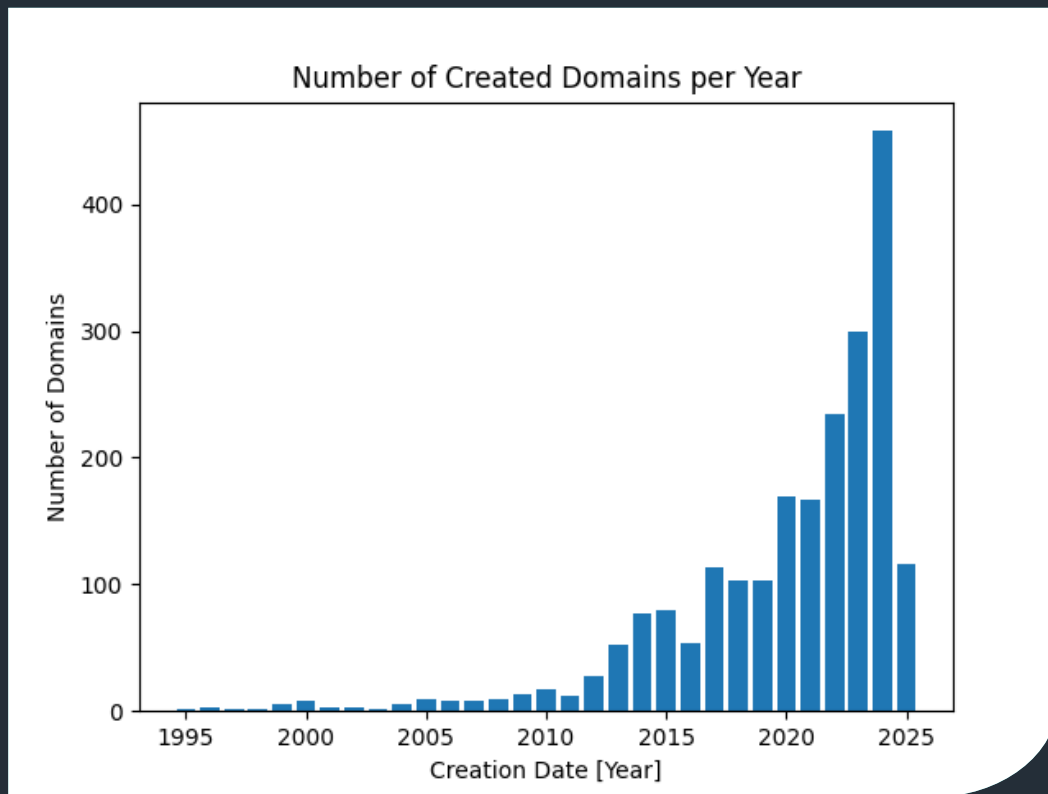
The Hidden Infrastructure Behind MediPhantom

- Payment Gateways
 - 60 unique domains
 - 35 HTML templates
- Live chat systems
 - LiveZilla, SmartSupp
 - Custom-built platform
- Phone numbers
- Fake pharmacy domains
 - 5,000 detected
 - Various languages



The Hidden Infrastructure Behind MediPhantom

- Domain growth trends
 - Exponential increase
 - Frequent domain rotation
- SSL and hosting infrastructure
 - No certificate reuse
 - Let's Encrypt, Sectigo and GTS
 - Various hosting providers:
 - OVHcloud, Cloudflare
 - Phaselayer.com, Pro-spero.ru, Proton66.ru, ...
- Many domains under single IP



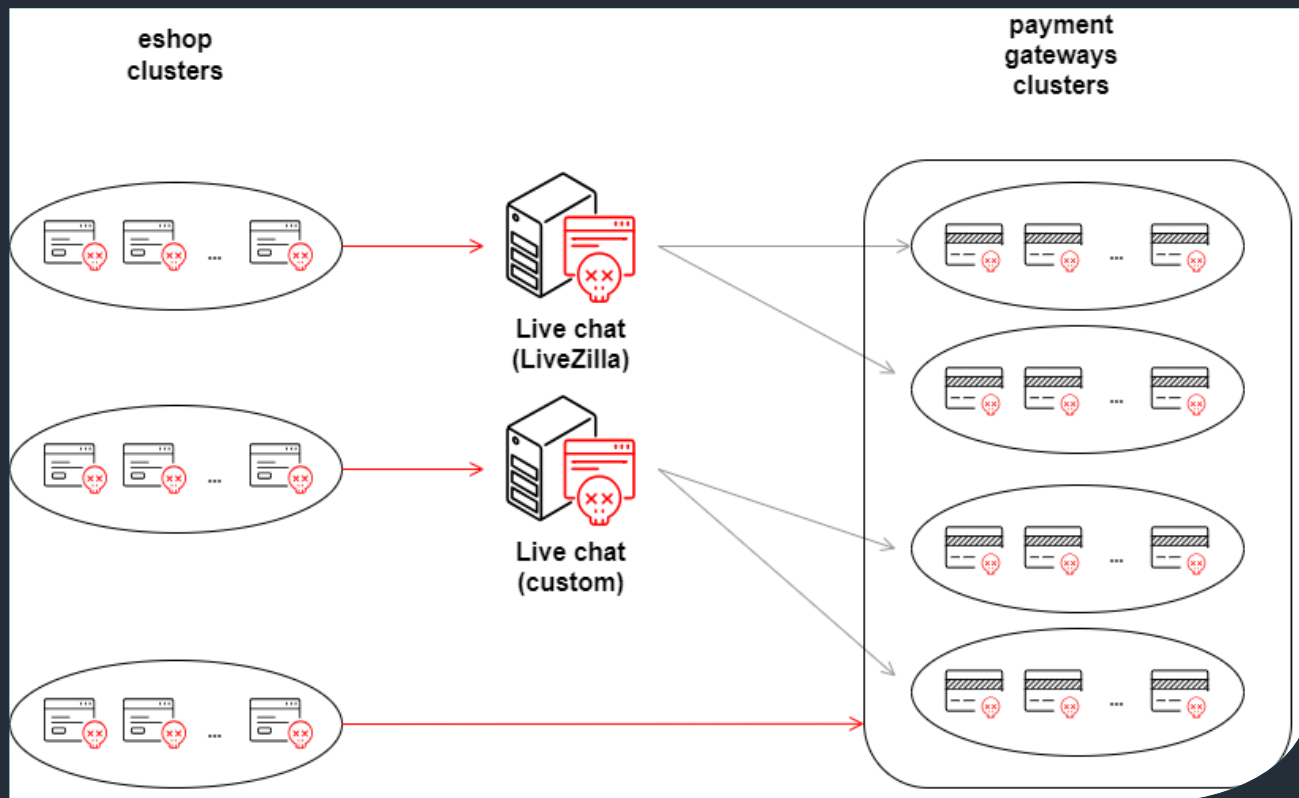
MediPhantom: One Group, Thousands of Faces



MediPhantom: One Group, Thousands of Faces

Live Chat & Payment Gateway Systems

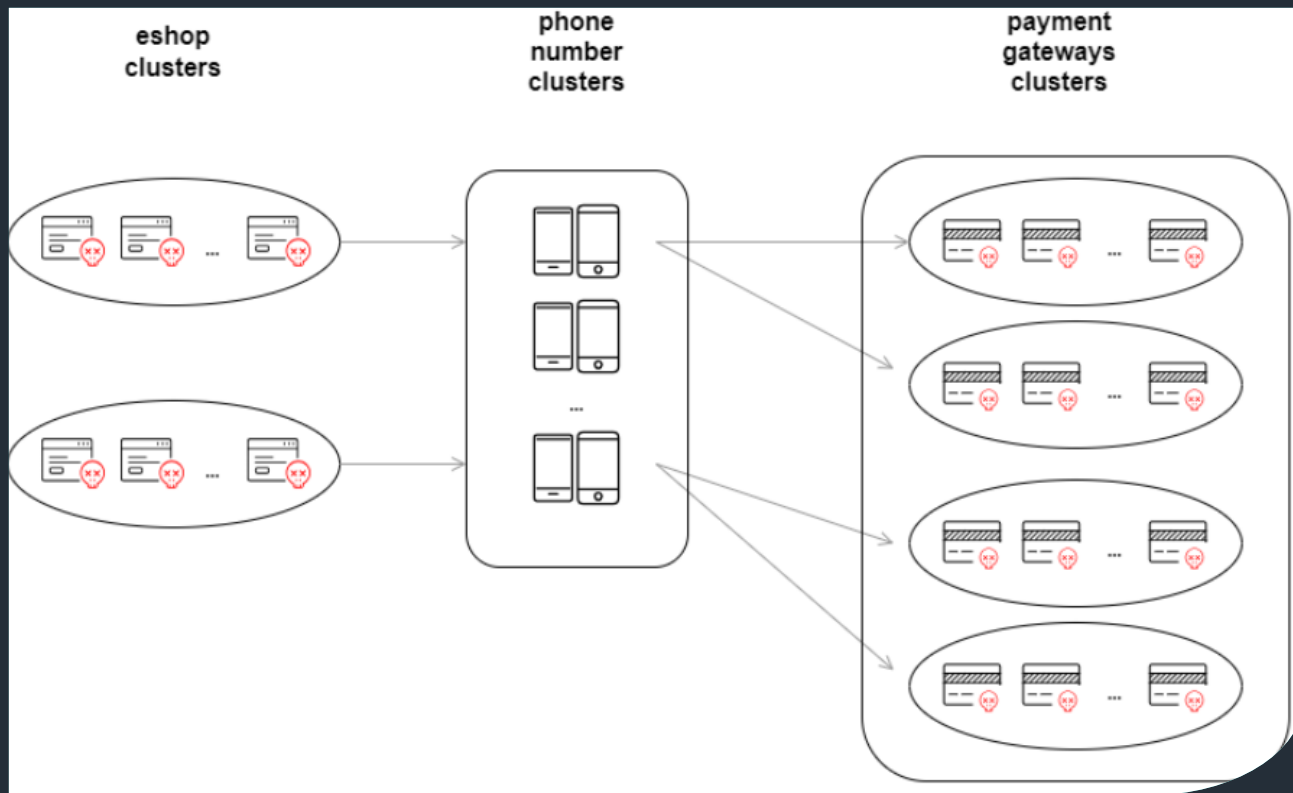
- Exclusive live chat
- Distinct clusters made of live chats
- Payment gateways formed into groups
- Live chat OR associated payment gateways
 - Operated by single threat actor



MediPhantom: One Group, Thousands of Faces

Phone Numbers

- Always present even if no Live Chat
- Many phones identified
- Identified phone number
 - Fake pharmacy by single threat actor





How We Can Fight Back: Detection and Defense Tactics

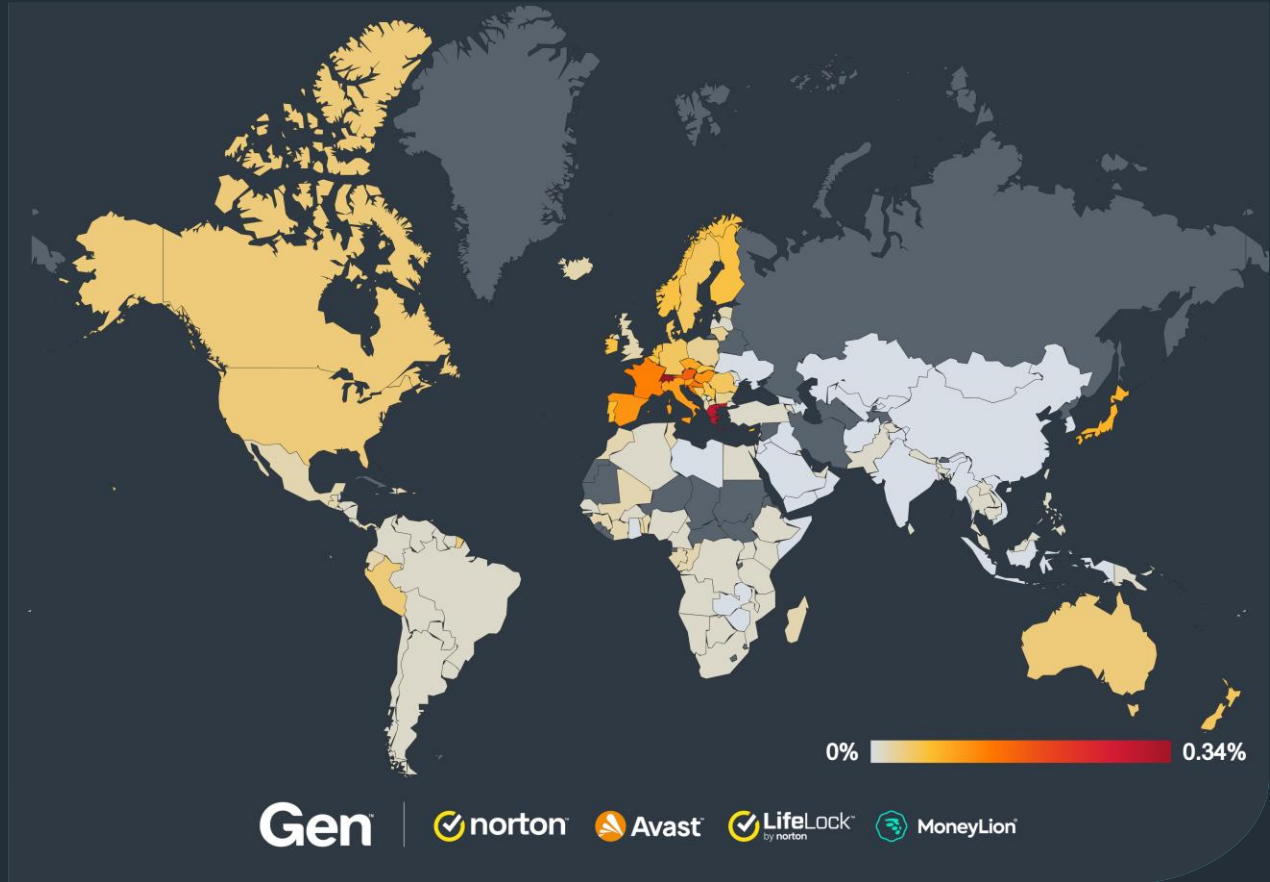
How We Can Fight Back: Detection and Defense Tactics

- Static Analysis
 - Source codes – detecting pharmacy brands (effective)
 - Only minor technical artifacts were shared across dozens of pharmacy brands:
 - Recurring patterns in JavaScript, CSS, and image names and paths
 - JavaScript implementation of Live Chat support
 - Fake embedded payment gateways, phone numbers
 - Likely a shared toolkit for the deployment process
- Network-Based Detection
 - Monitoring redirections to known fraudulent payment gateways
 - Feedback loop – Newly extracted IoCs fed back to the detection pipeline

Tracking the Threat: What the Data Reveals

Geographic distribution

- Primarily targeting:
 - Europe
 - Greece, Croatia, Hungary
 - Switzerland, Austria
 - France, Spain
 - Japan & Australia
 - USA & Canada
- Localization
 - 25 languages



Key Takeaways

- It's not just about cybersecurity (scams, fraud, ...), it's about public health
- Fake pharmacies are not isolated scams, global problem
- Tracked as a specific group – MediPhantom
- The operation is socially and technically sophisticated, manipulative
- Raising awareness and education
- What users can do:
 - Always verify the pharmacy's legitimacy, learn how
 - Trust your local providers, prescriptions are in place for a reason
 - Be skeptical and beware of “Too good to be true” offers
 - Reputable AV can protect you!

Thank you

Ľuboš Bever

Threat Analysis Engineer
lubos.bever@gendigital.com

Jan Rubín

Threat Research Team Lead
jan.rubin@gendigital.com



References

- [1] Harvard Health Publishing. (2023, August 1). Don't get duped: Here's how to avoid online pharmacy risks. Harvard Health.
<https://www.health.harvard.edu/staying-healthy/dont-get-dupedheres-how-to-avoid-online-pharmacy-risks>
- [2] Centers for Disease Control and Prevention. (2024, October 2). Potential public health risk among individuals ordering counterfeit prescription medications from online pharmacies.
<https://www.cdc.gov/media/releases/2024/s1002-counterfit-prescription-online-pharmacies.html>