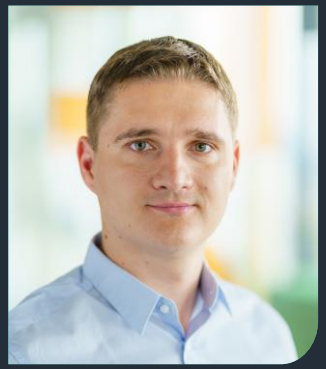
The Dark Prescription:

Inside the Infrastructure of Illegal Online Pharmacies

24 Sept. 2025

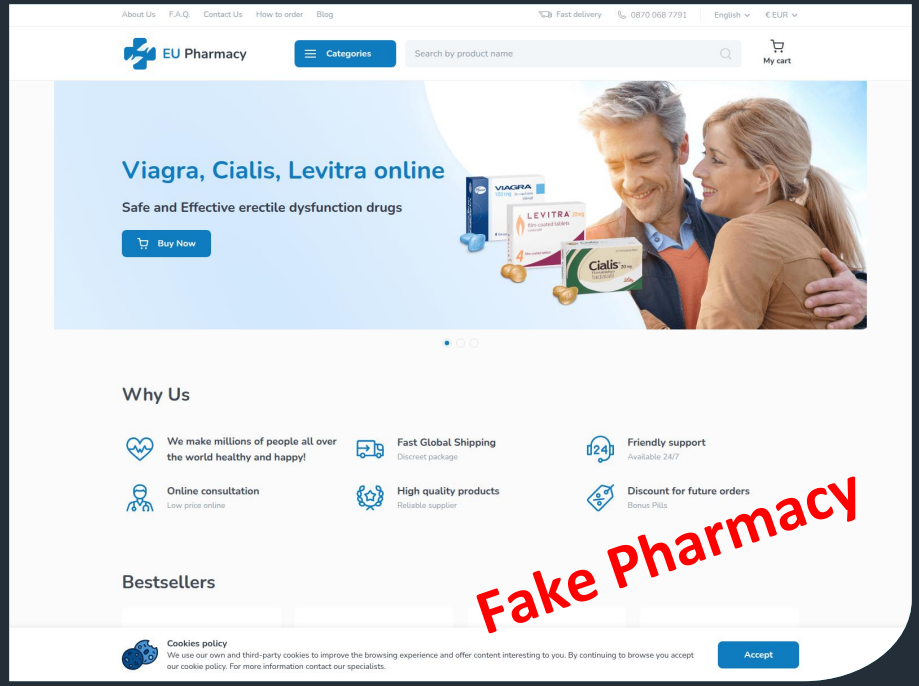
Hello, Berlin!

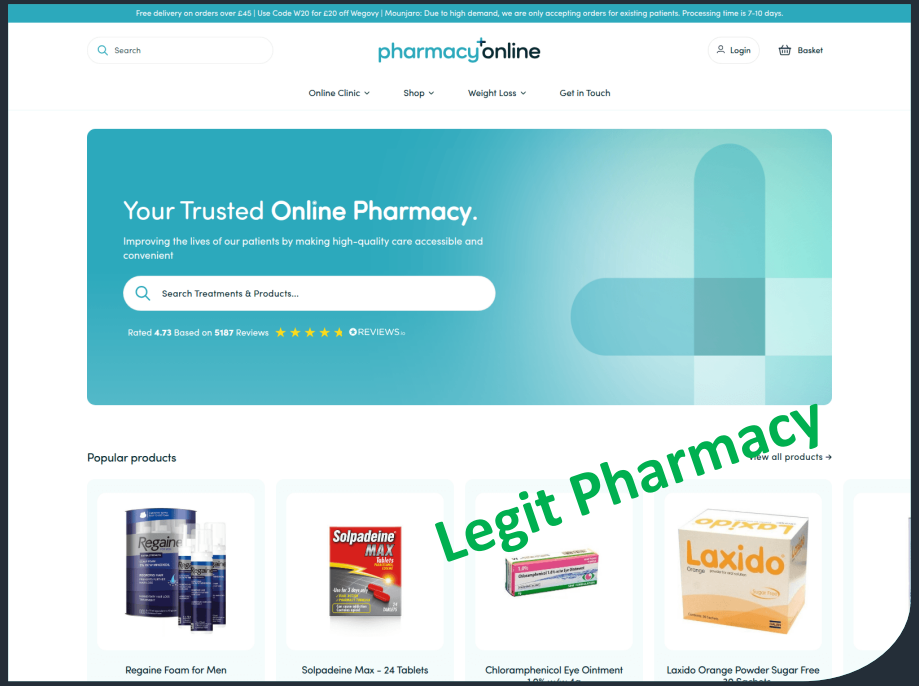
- Ľuboš Bever
- Threat Researcher
- Member of Threat Intelligence team
- Focusing on scams
  - Fake e-Shops and PDF threats
- SimRacing in free time



- 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

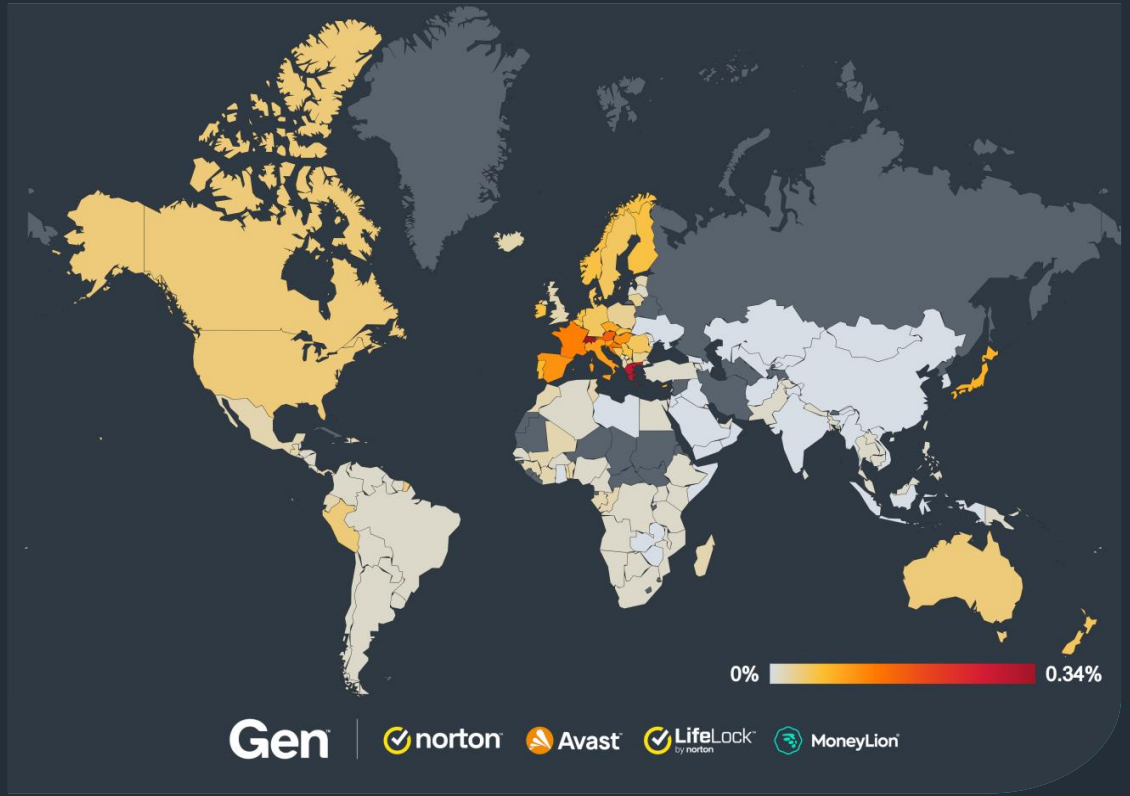
Can You Spot the Scam?





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.



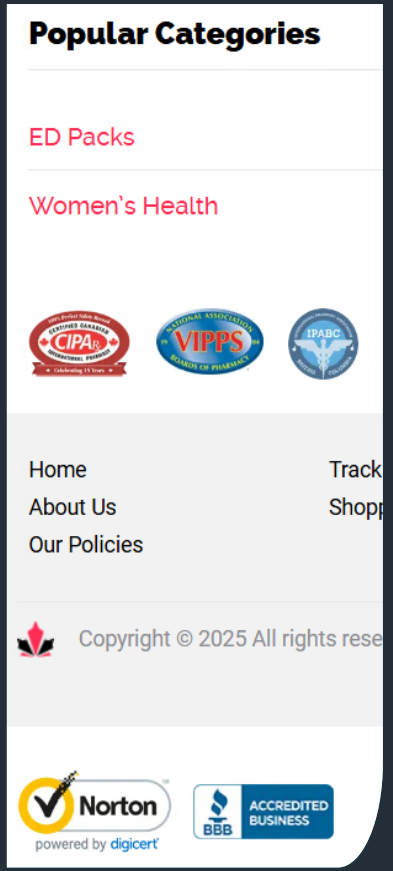
The Digital Drug Market: Who's Selling, Who's Scamming

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:

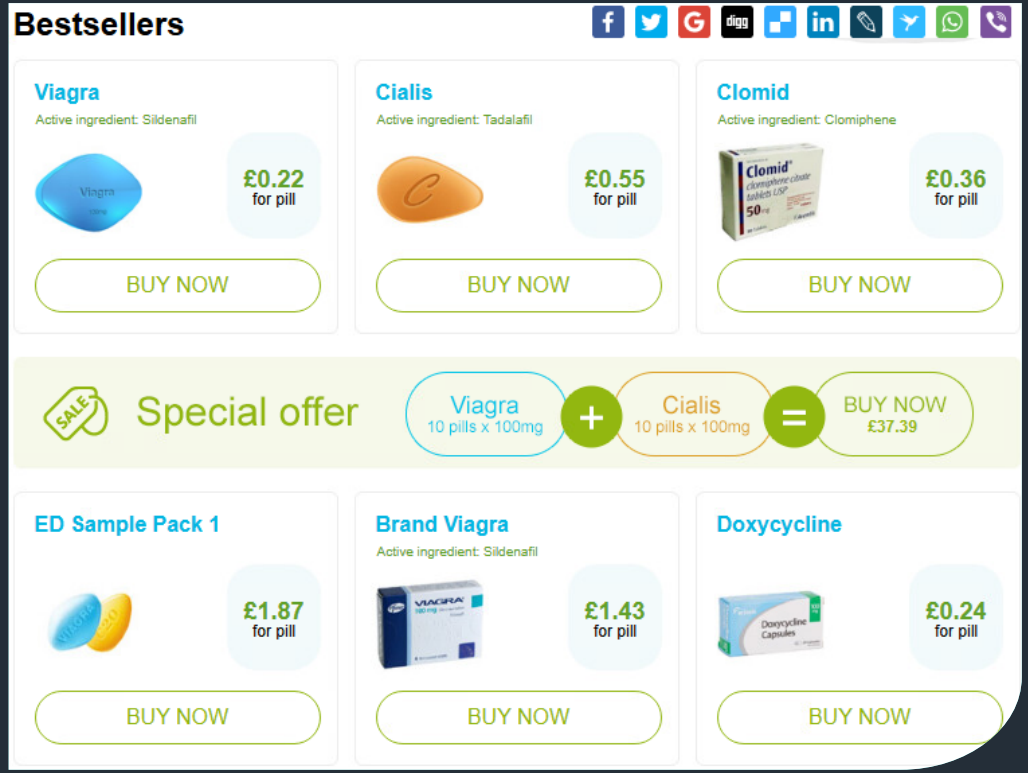
- False sense of legitimacy
- Fake badges and logos
- Cheap prescription pills without prescription
- Overly positive or generic customer reviews
- Fake payment gateways



How Victims Are Targeted: MediPhantom in Action

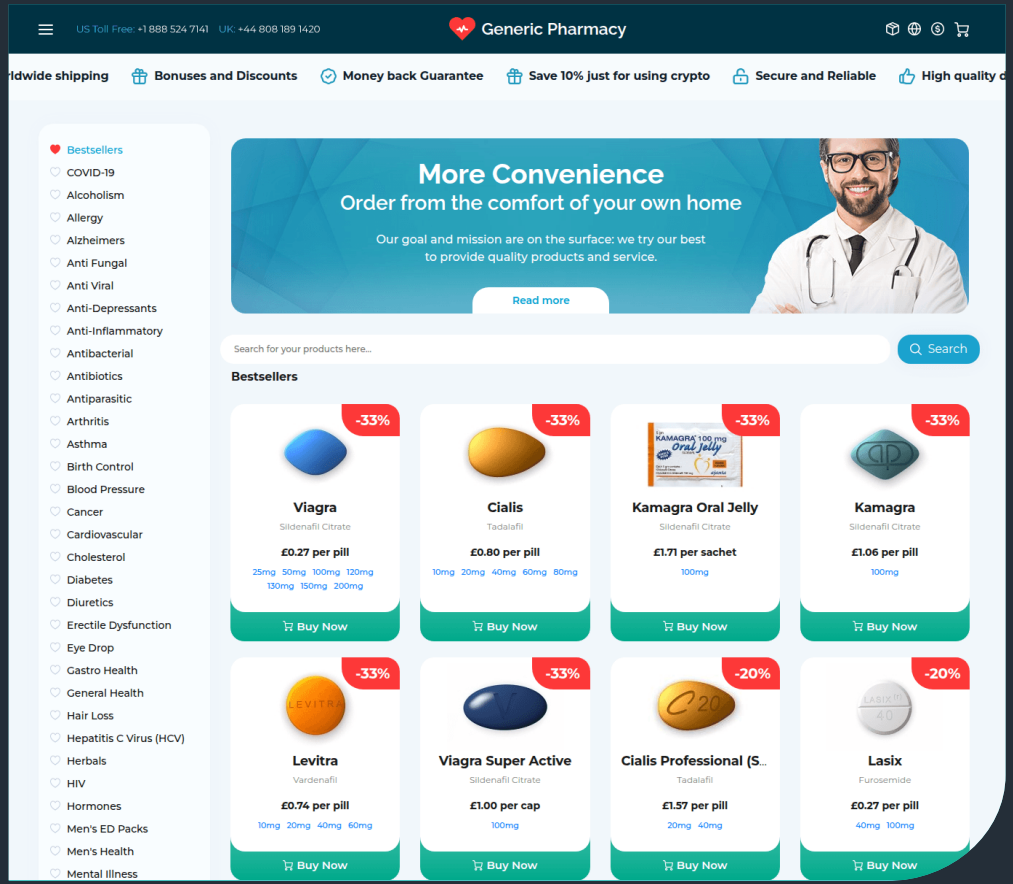
Finding the Vulnerable: How Victims Are Selected

- 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



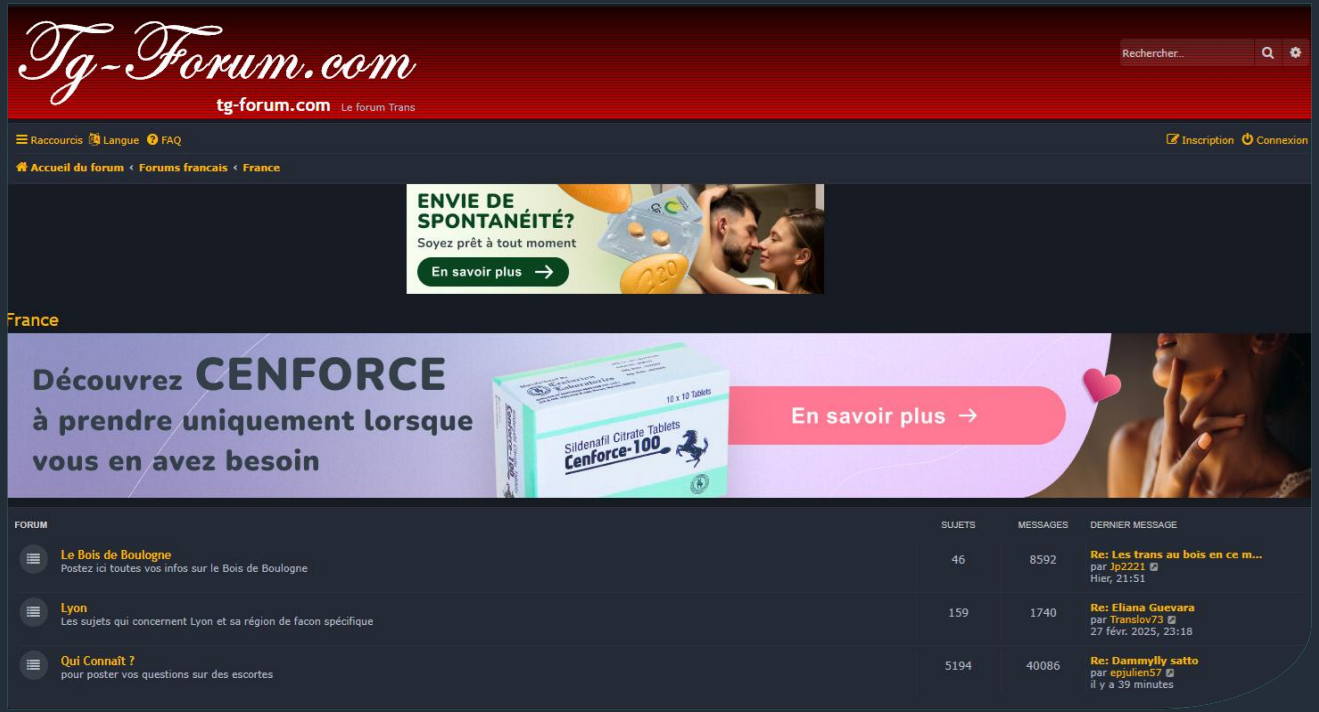
Crafting the Trap: From Scam Setup to Link Drop

- 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



Crafting the Trap: From Scam Setup to Link Drop

Active Delivery Methods

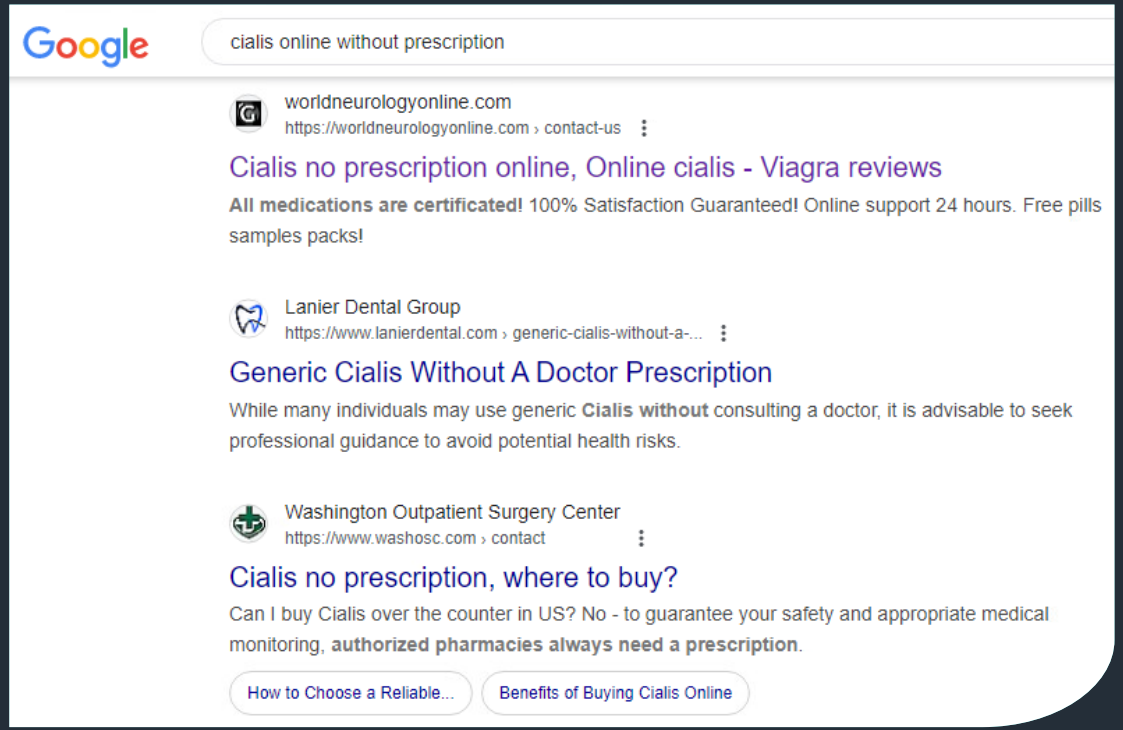


Online Advertisements
Banner ads

Crafting the Trap: From Scam Setup to Link Drop

Passive Delivery Method — SEO Manipulation

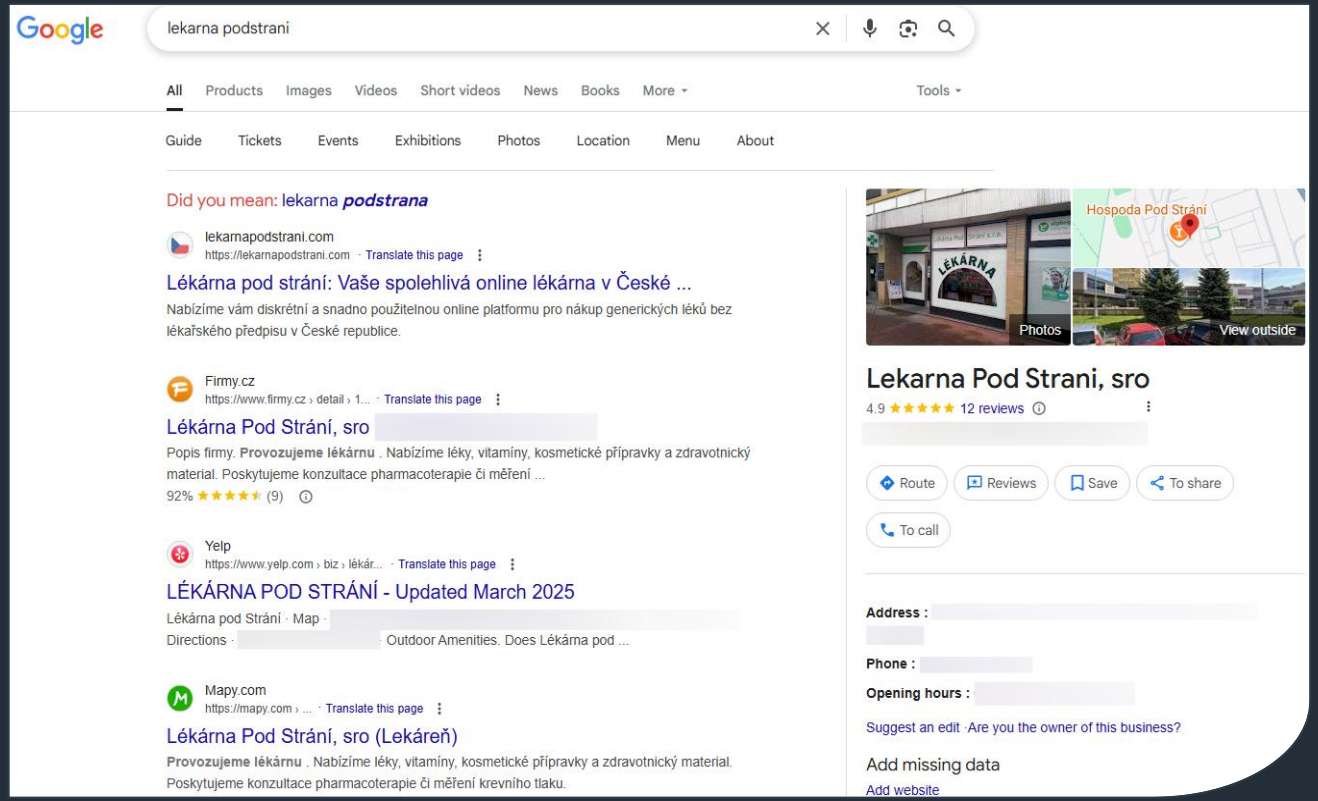
- Users actively searching for medications
- Require unauthorized access
- Crawler-bots are confused
- Injection of:
  - Redirection to pharmacy
  - Deceptive content on compromised domain
- Illusion of legitimacy



Crafting the Trap: From Scam Setup to Link Drop

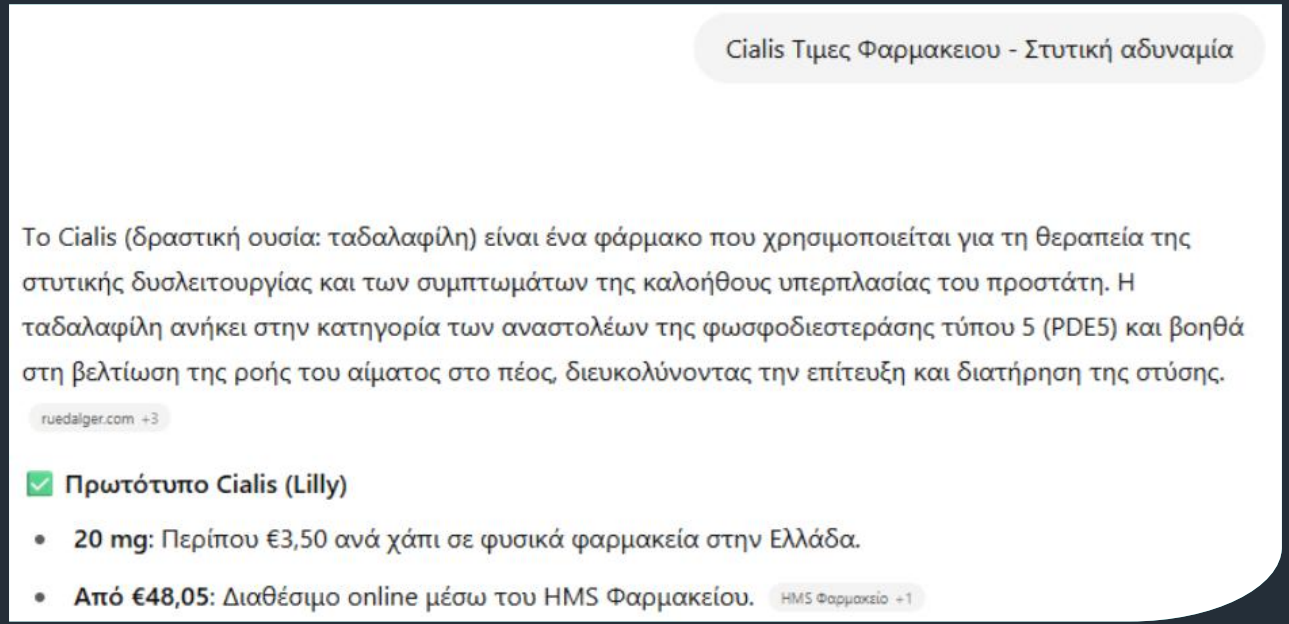
Passive Delivery Method — SEO Manipulation

Brand impersonation
Mimicking a real brand



Crafting the Trap: From Scam Setup to Link Drop

Passive Delivery Method — SEO Manipulation

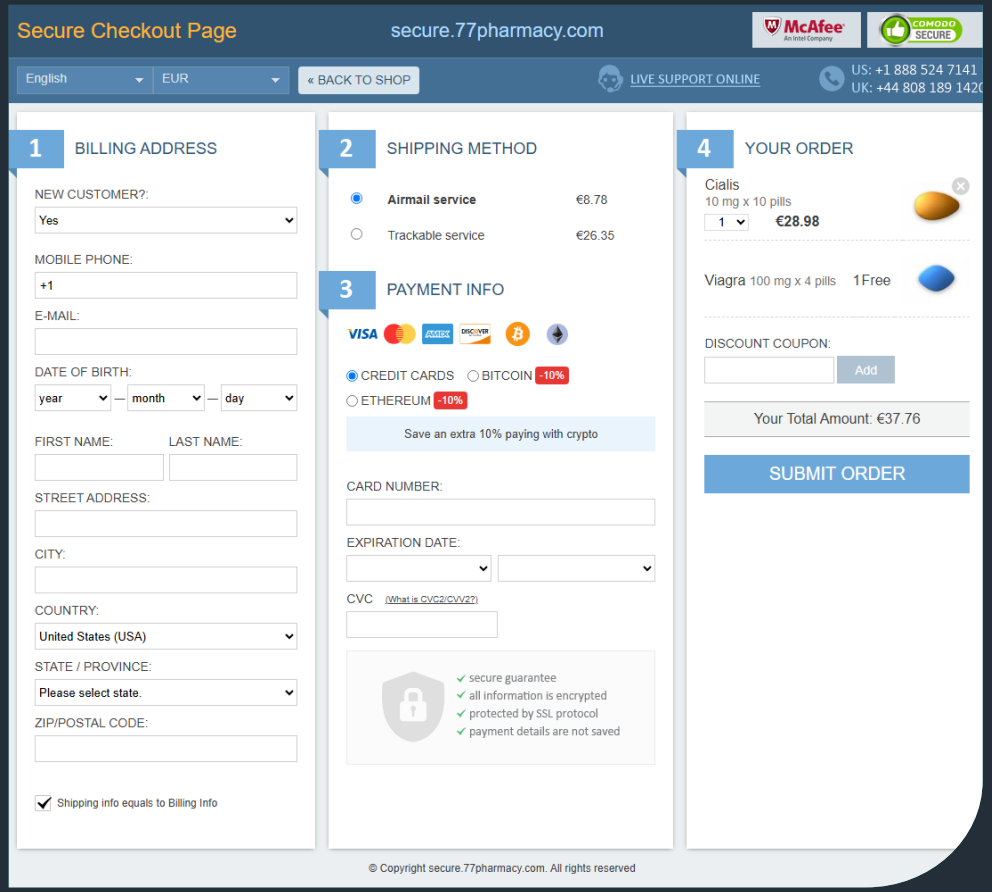


Poisoned Chatbot

“Cialis Pharmacy Prices – Erectile dysfunction”

The Click That Costs: When the Scam Hits

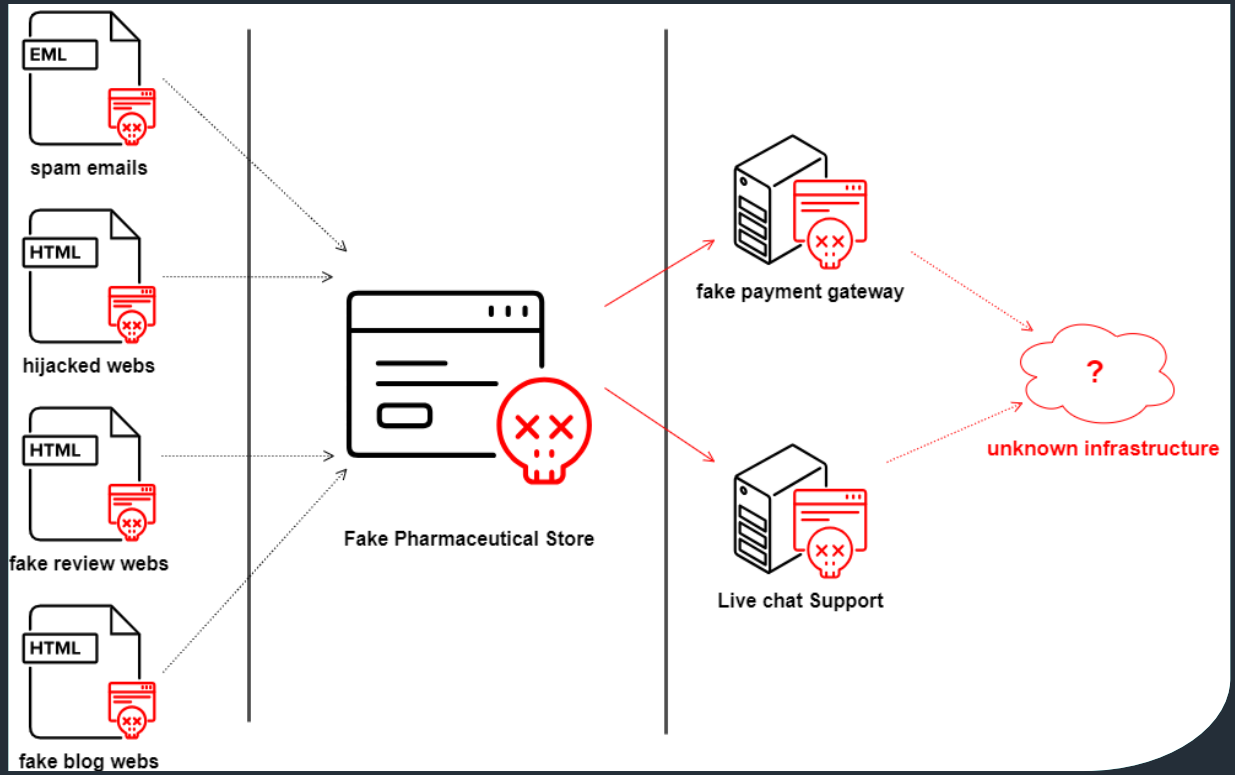
- Typical shopping workflow
- Not secure payment gateway
  - Often separate domain
  - Attackers fully control
- Solicited sensitive details:
  - Date of birth
  - Medical anamnesis
- Customer support:
  - Live chat & phone numbers



The Hidden Infrastructure Behind MediPhantom

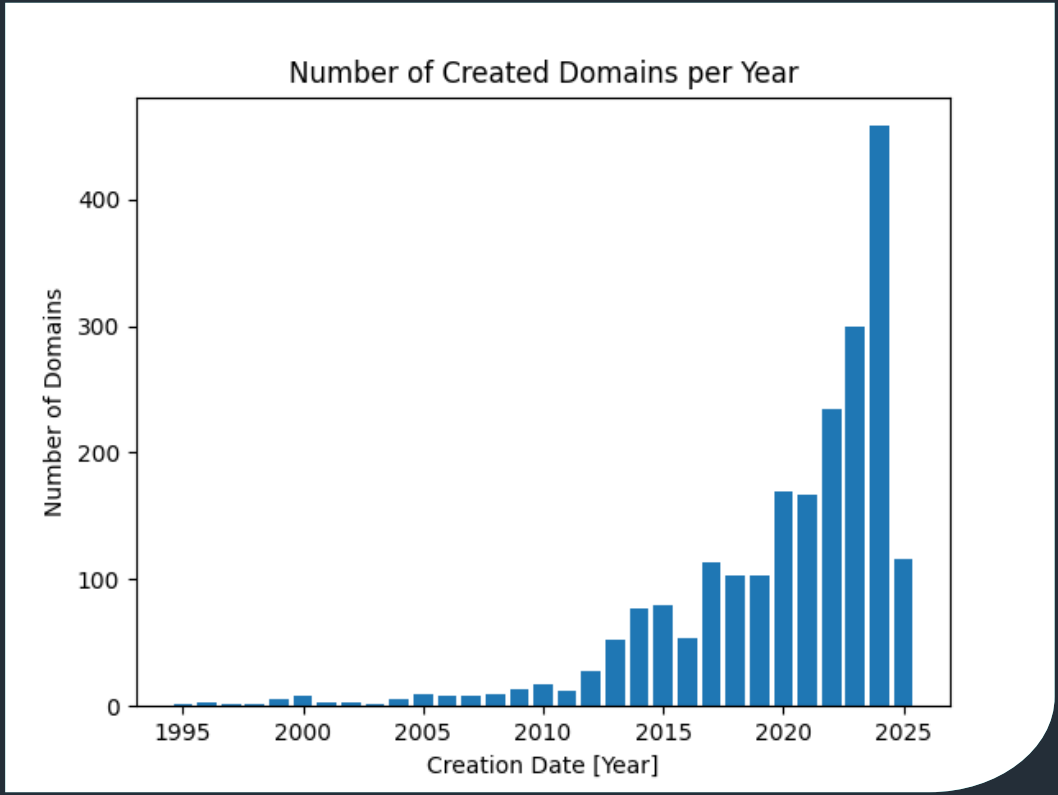
The Hidden Infrastructure Behind MediPhantom

- 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

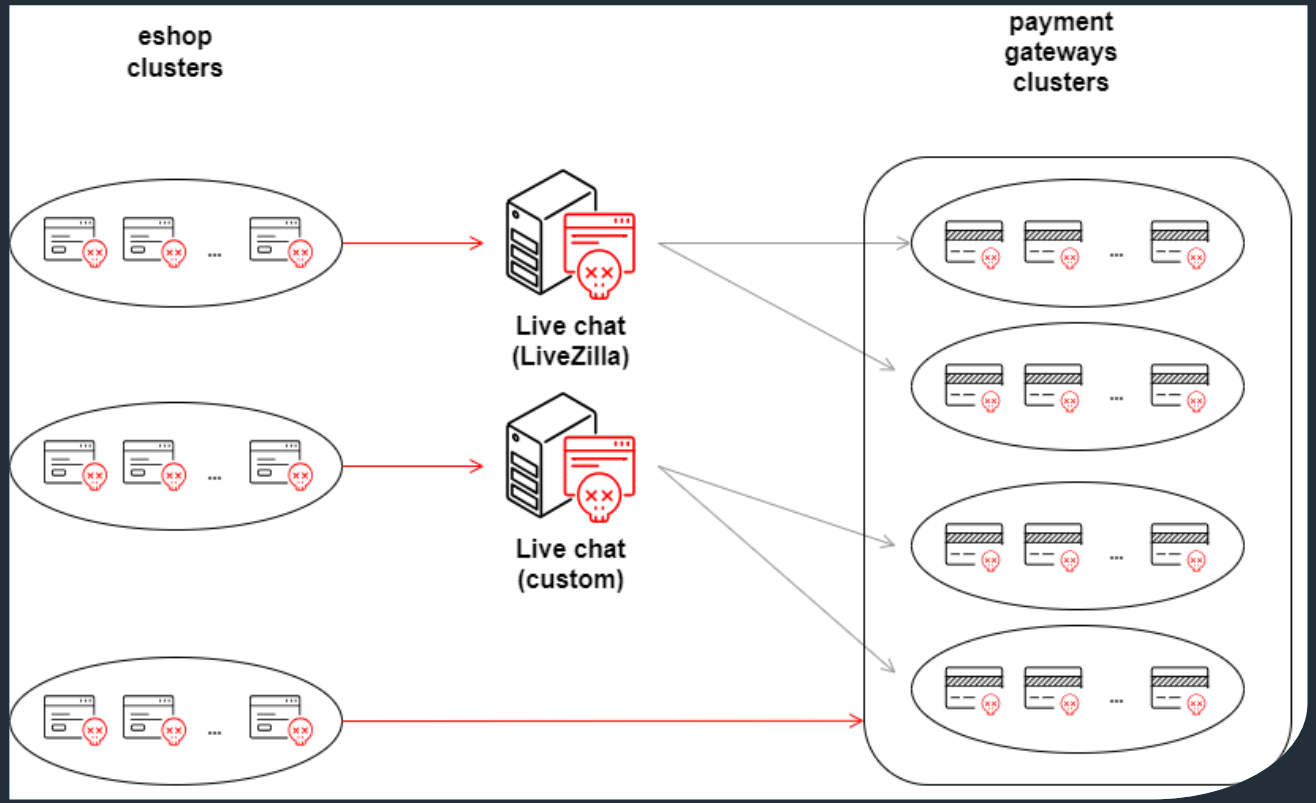


MediPhantom: One Group, Thousands of Faces

MediPhantom: One Group, Thousands of Faces

Live Chat & Payment Gateway Systems

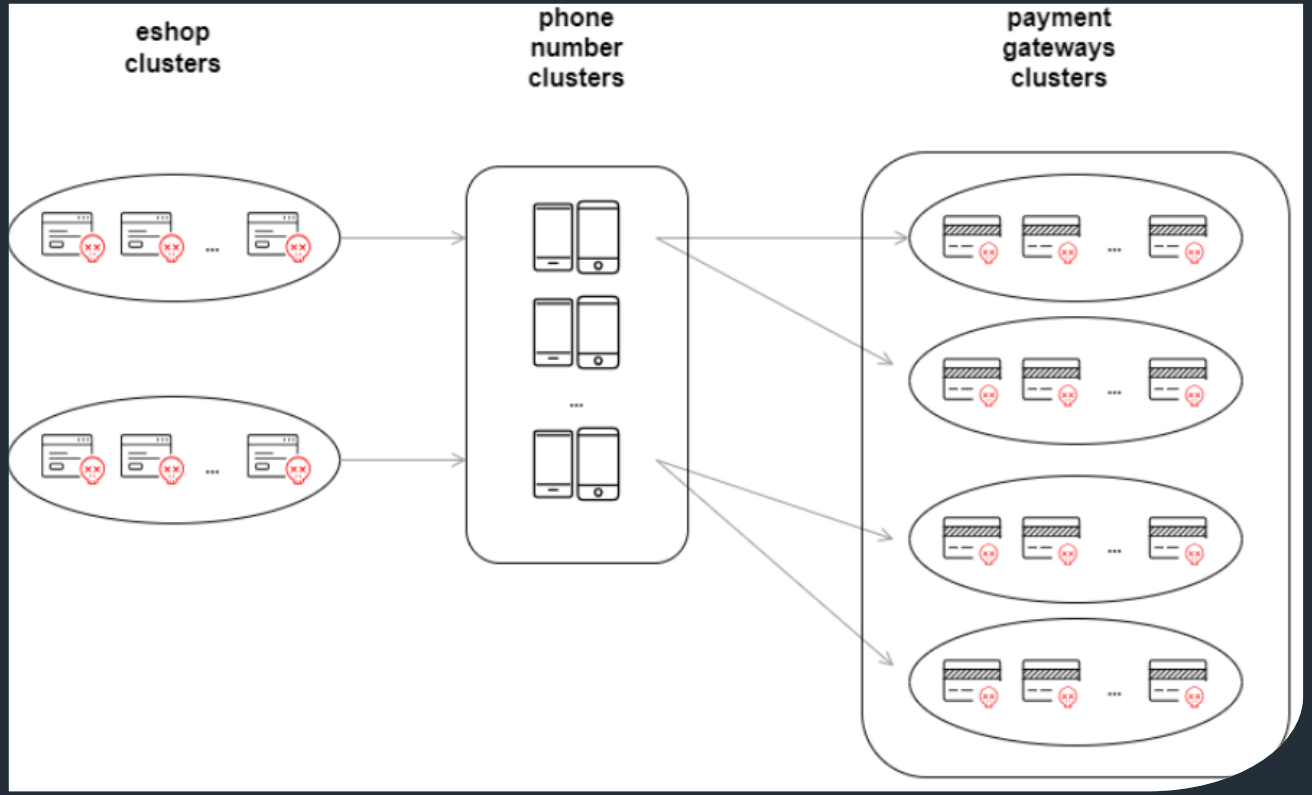
- Exclusive live chat
- Distinct clusters made of live chats
- Payment gateways formed into groups
- Live chat OR associated payment gateways
  - Operated by single threat actor



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

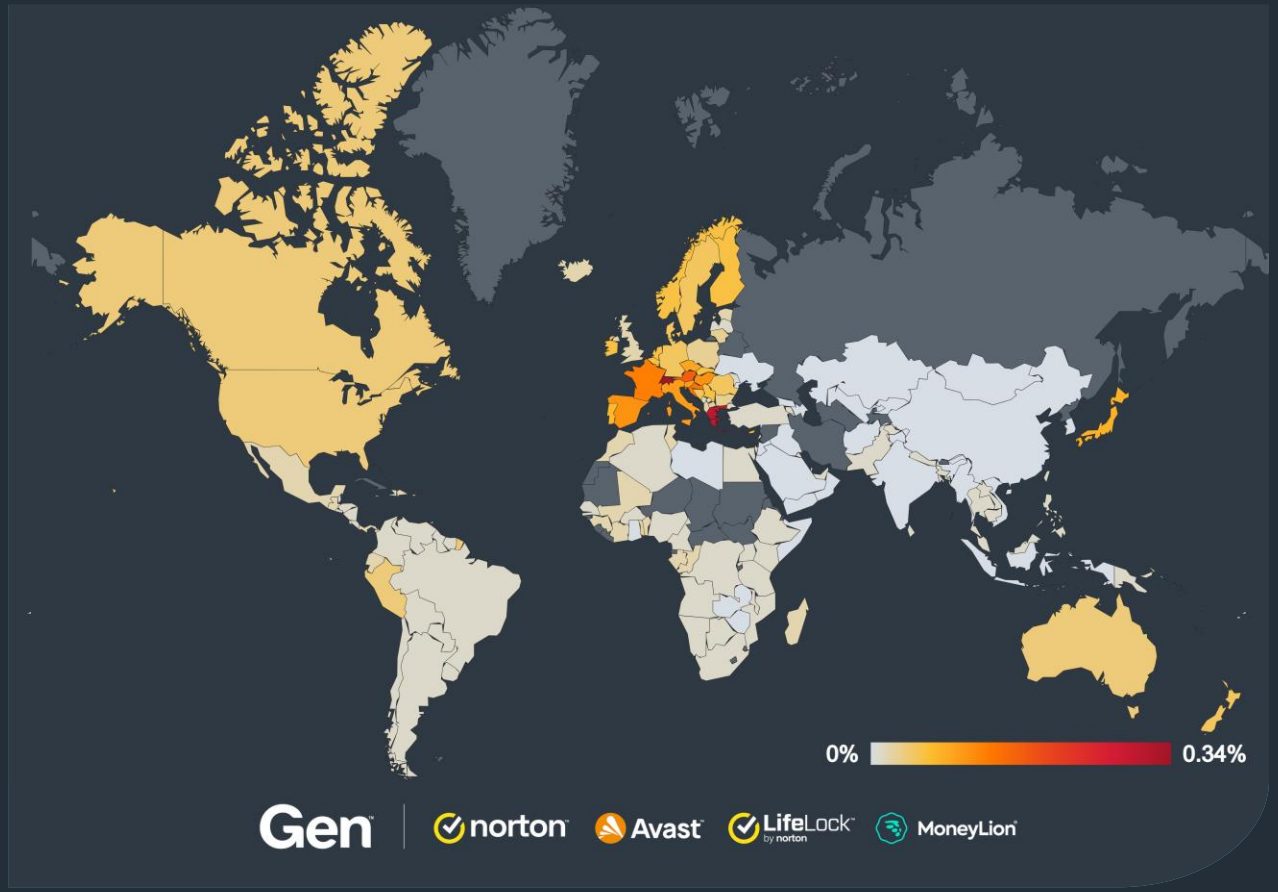
How We Can Fight Back: Detection and Defense Tactics

- 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



Gen

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

Gen™

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