**Raport de investigare a infrastructurii IT**

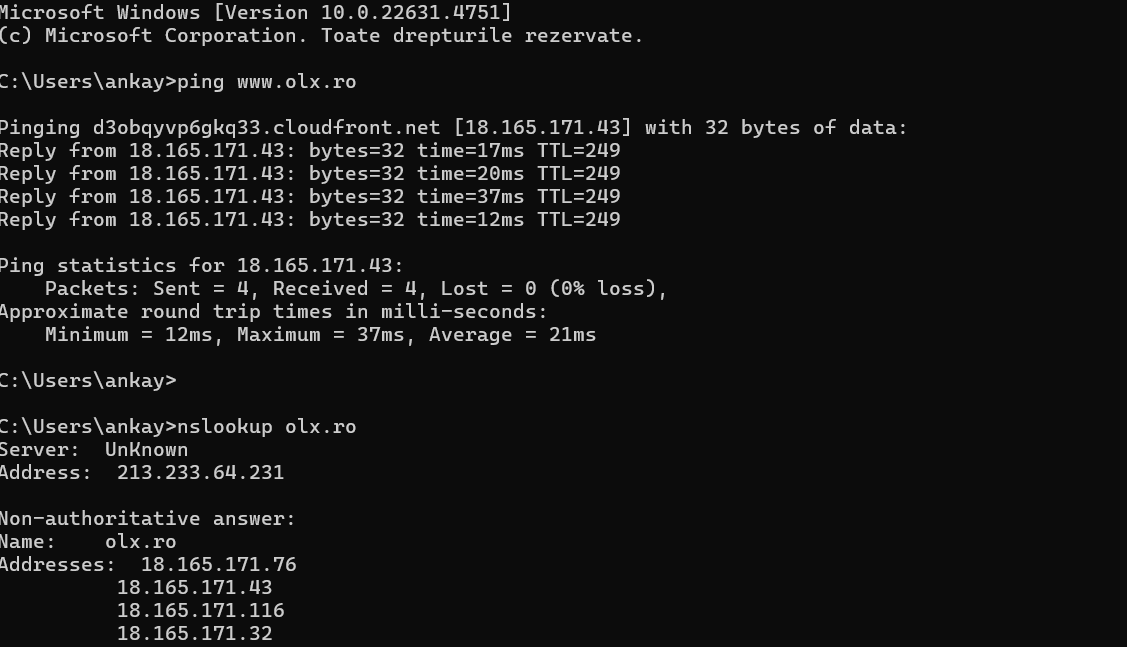
**Introducere**

Acest raport detaliază rezultatele unei investigații asupra infrastructurii IT a organizației OLX. Investigația a fost realizată folosind instrumente precum Shodan, OSINT Framework și alte surse disponibile public.

**Metodologie**

 **Ping și identificarea locației IP.**

* Comanda ping a fost utilizată pentru a verifica conectivitatea.
* Nslookup pentru afisarea adresei IP



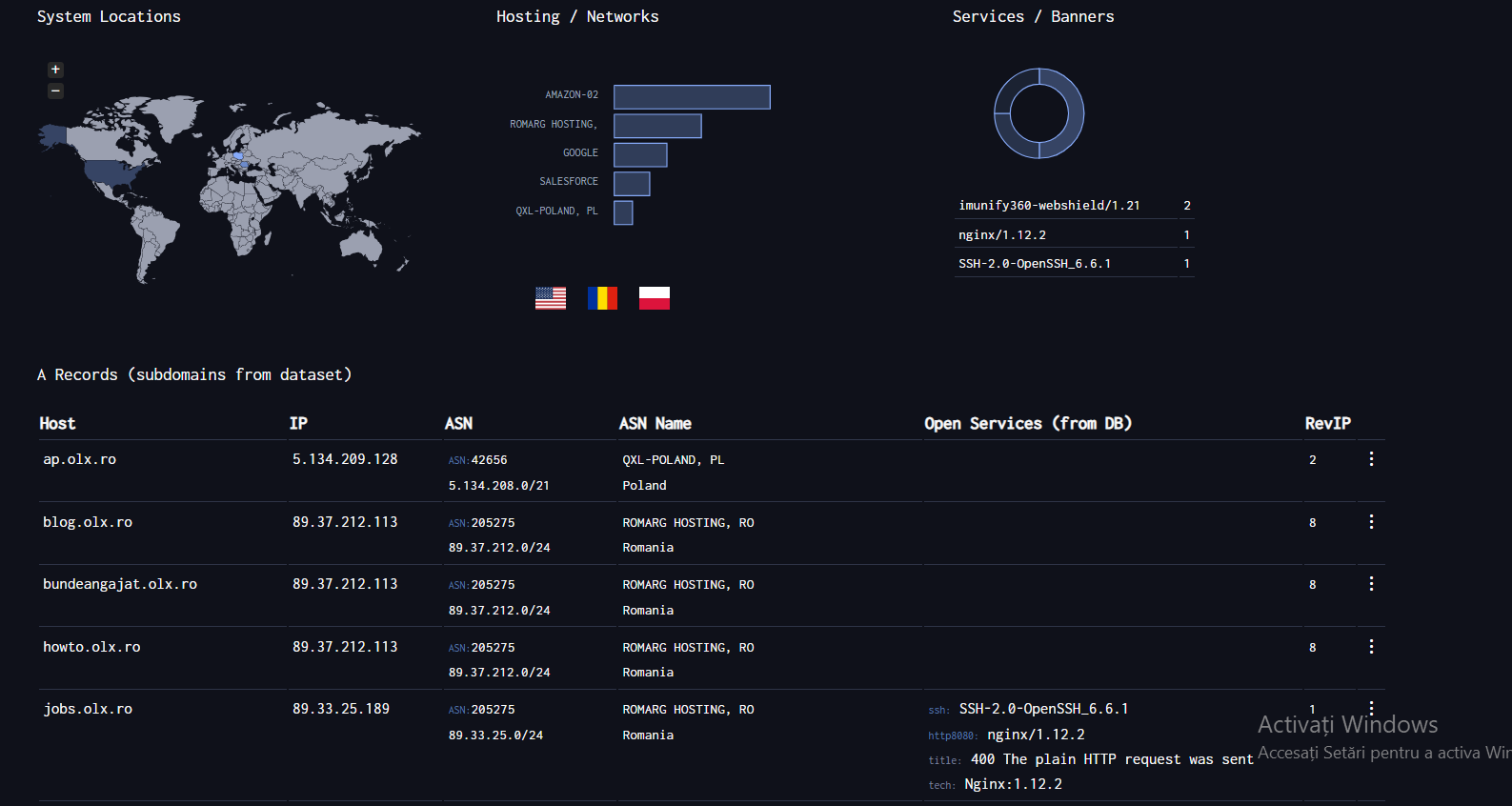
 **Scanarea DNS și căutarea subdomeniilor.**

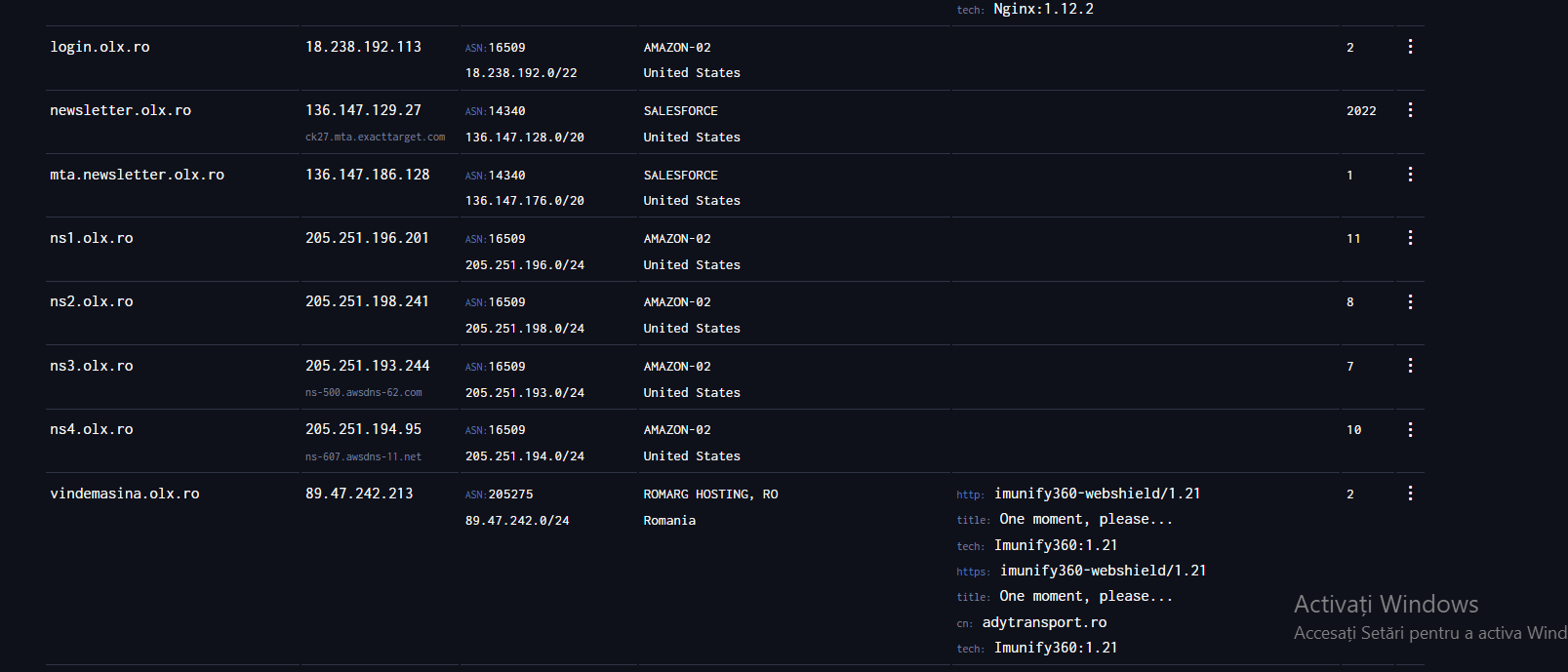
* DNS Dumpster a fost folosit pentru a analiza subdomeniile asociate.

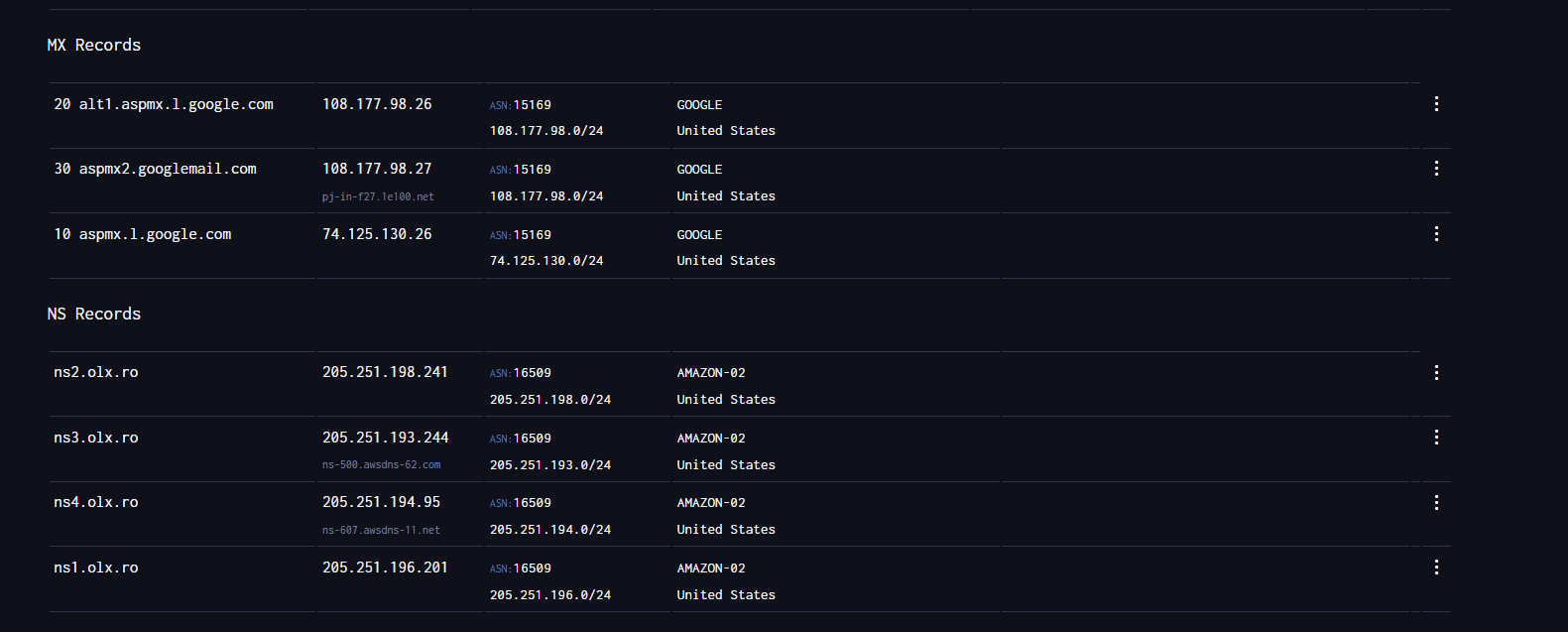
 **Căutare Shodan.**

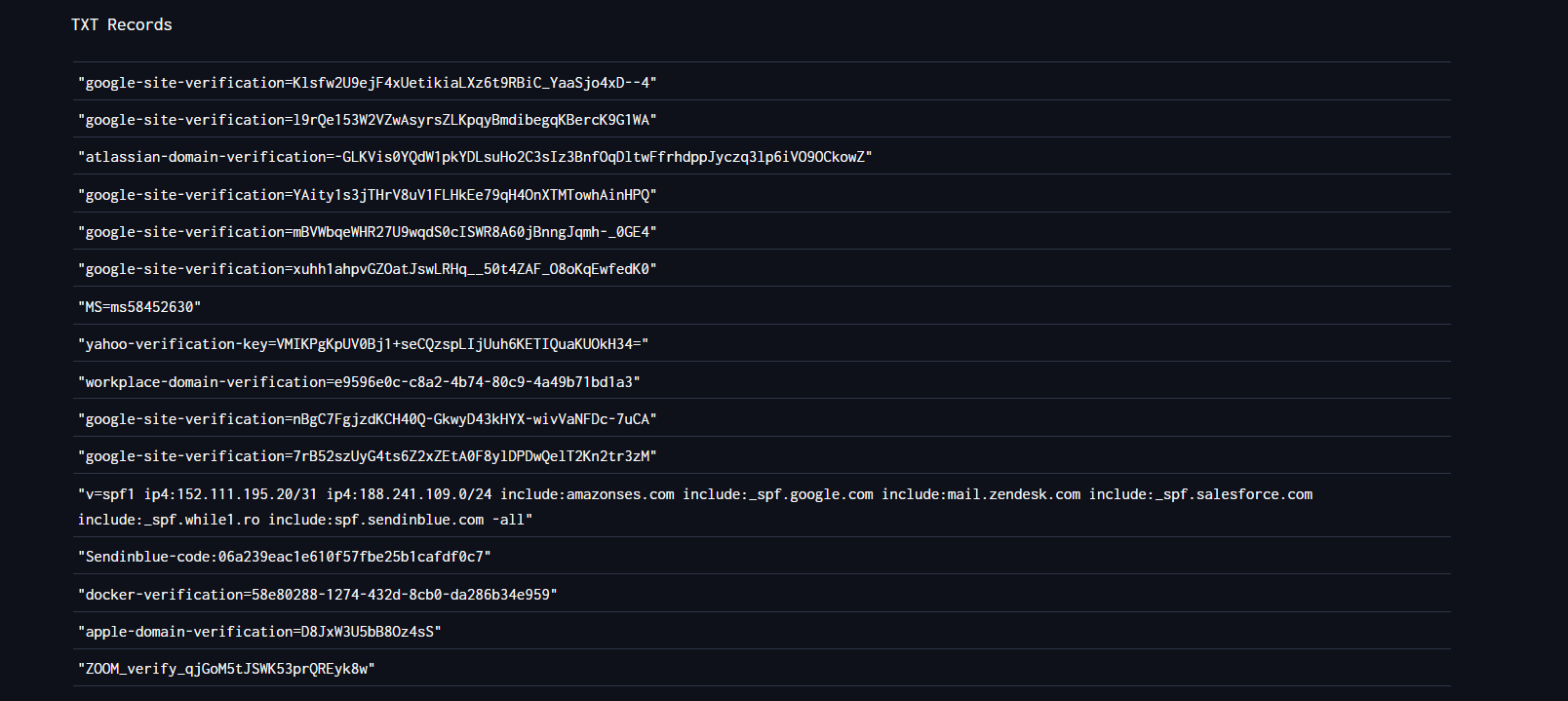
* Shodan a fost folosit pentru a colecta informații despre serviciile și porturile active.

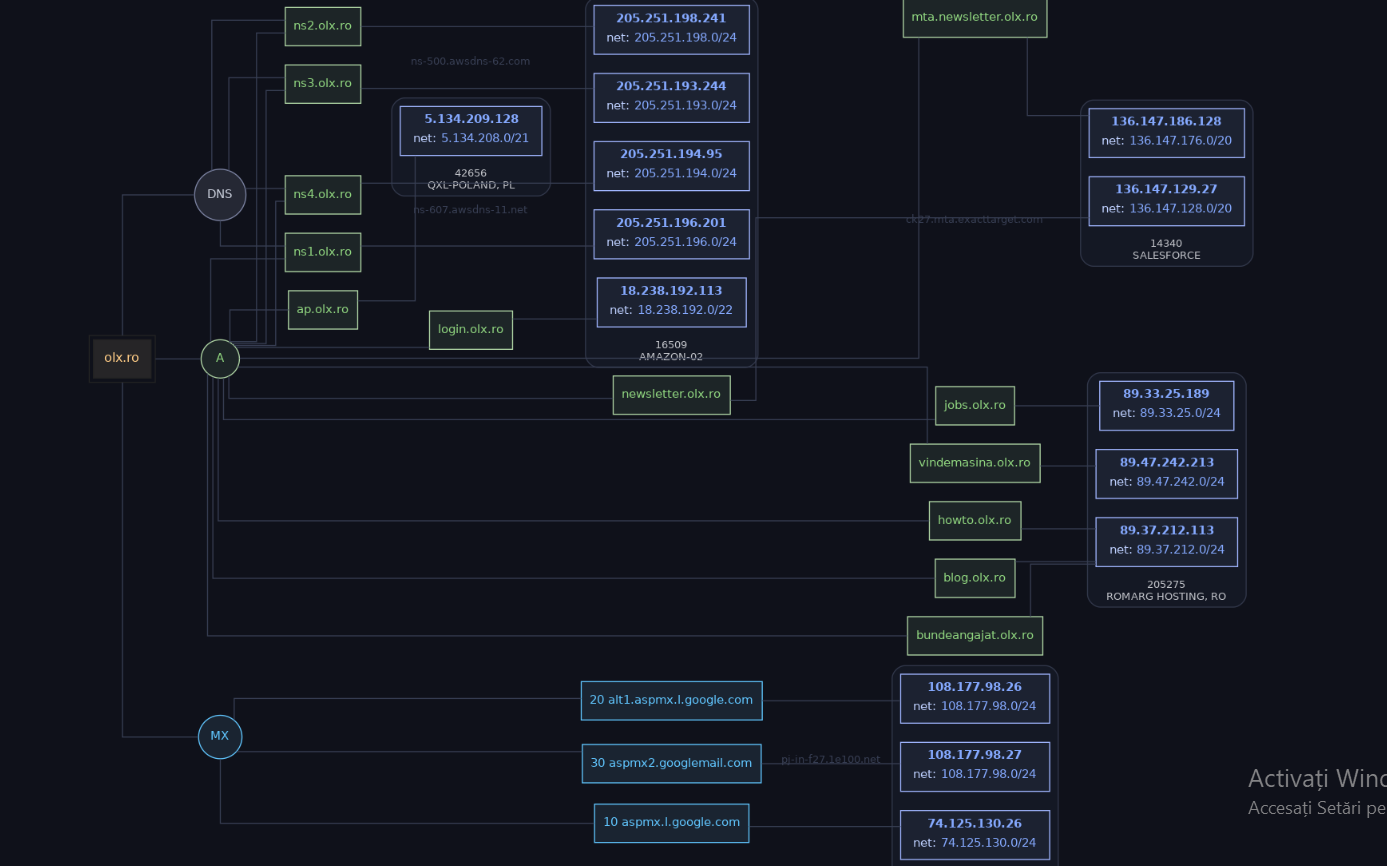
**Datele colectate**

**Rezultatele cautarii cu DNS Dumpster** 









Din aceste imagini pot observa următoarea structură a rețelei:

1. Hosting și Locații:

* Serviciile sunt găzduite în principal pe 4 provideri: Amazon, RoWeb Hosting, Google și Salesforce
* Există servere în mai multe țări: România, Polonia și Statele Unite
* Se folosesc mai multe subdomenii .olx.ro

1. Servicii identificate:

* Ubuntu/Linux cu imufy360-webshield
* Nginx 1.12.2
* SSH-2.0-OpenSSL

1. Structura DNS:

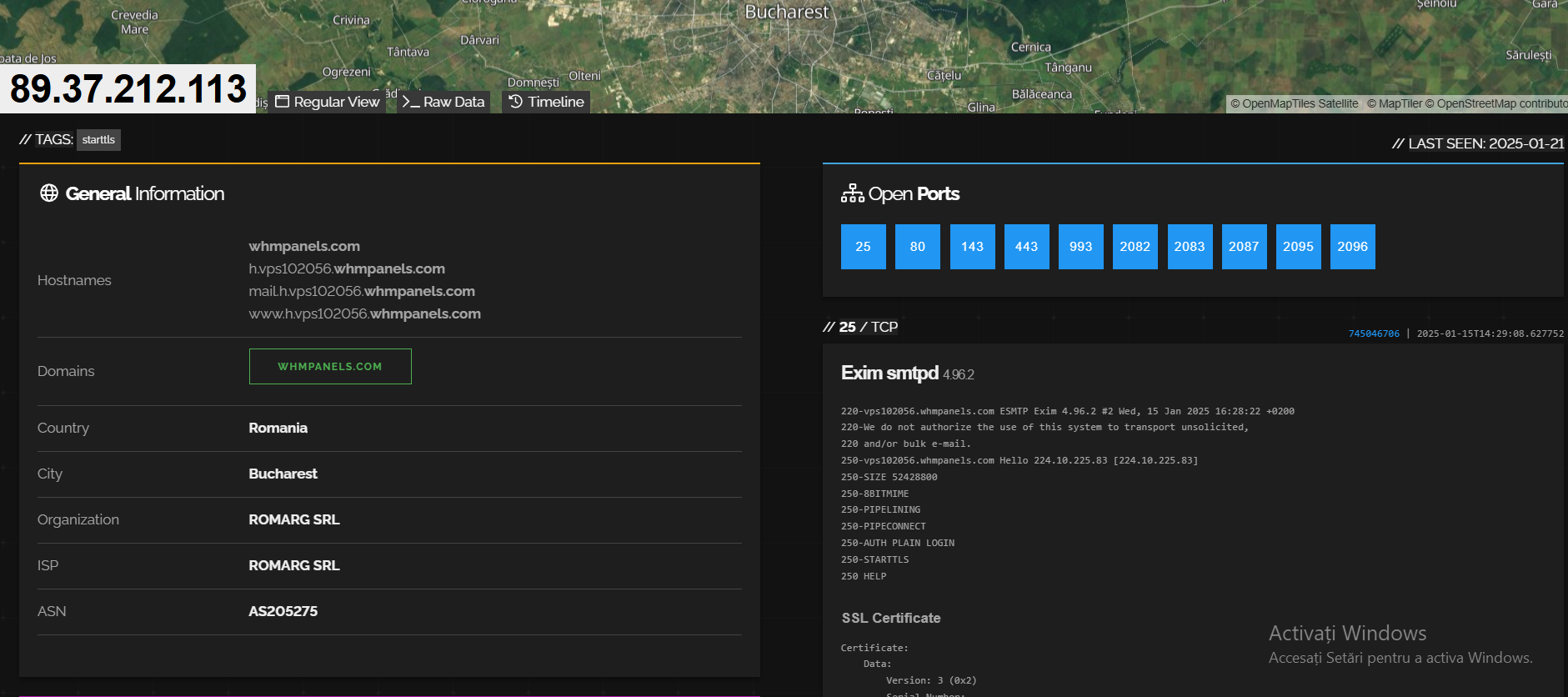
* Mai multe înregistrări A Records care mapează subdomenii către IP-uri specifice
* NS Records pentru servere de nume
* Înregistrări MX pentru mail servers (gestionate prin Google)
* Multiple înregistrări TXT pentru verificări de domeniu (Google, Atlassian, Yahoo, etc.)
* Configurare SPF care include servicii precum Amazon SES, Google, Zendesk, Salesforce

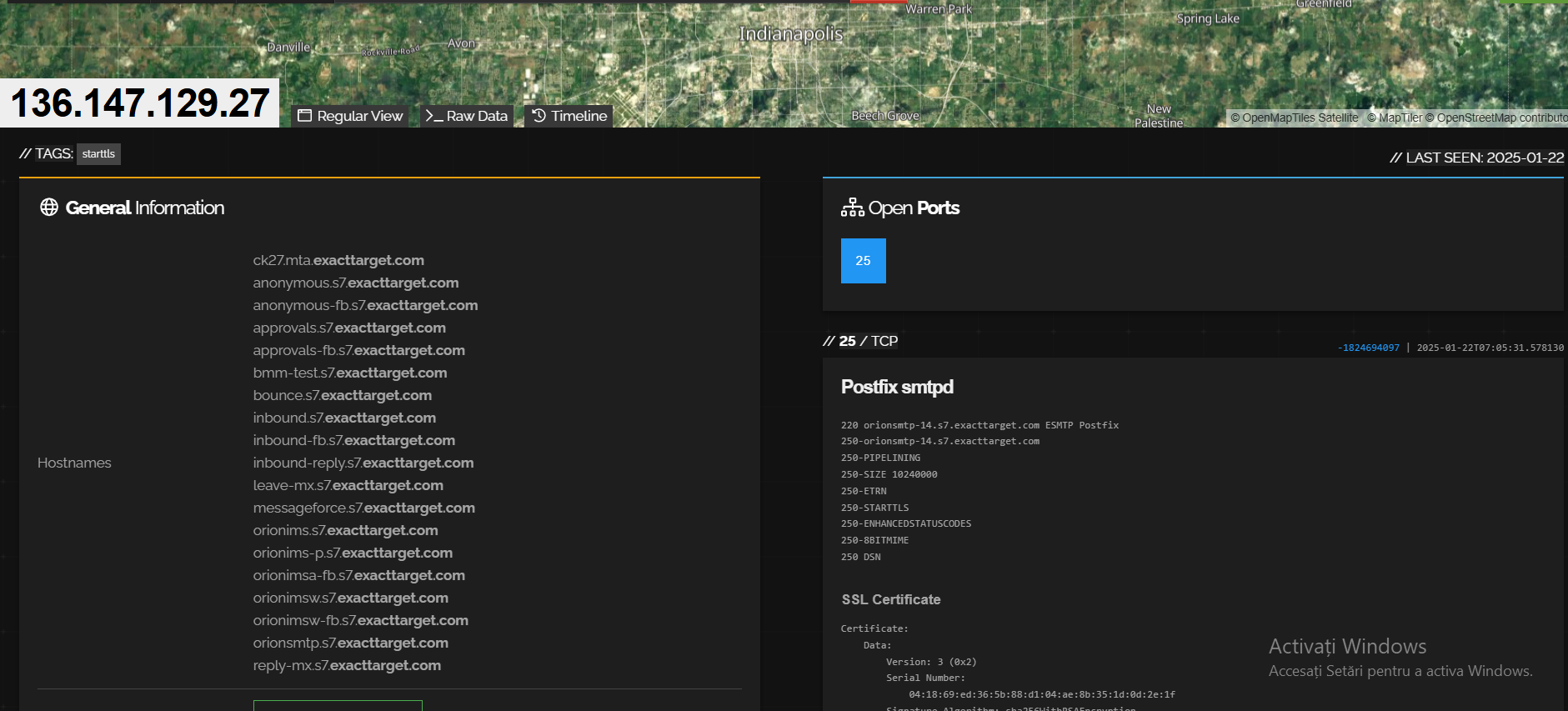
1. Securitate:

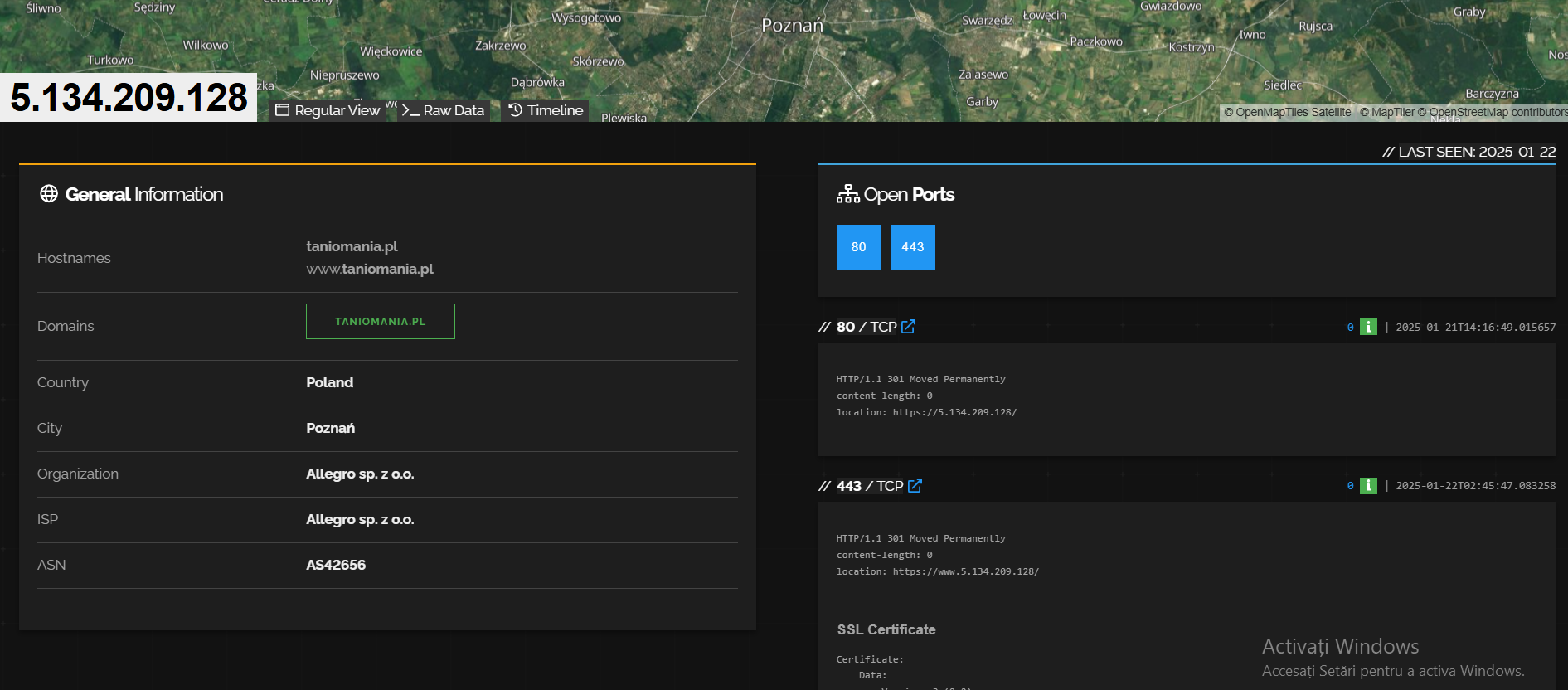
* Există verificări multiple de domeniu implementate
* Folosește imufy360 ca soluție de securitate
* Are configurate diverse servicii de verificare pentru diferite platforme

Rețeaua pare să fie una complexă, distribuită între mai mulți furnizori de servicii, cu accent pe scalabilitate și securitate. Are o prezență internațională și folosește servicii cloud de la furnizori majori pentru diferite componente ale infrastructurii.

**Analiza cu Shodan.io a unor adrese din locatii diferite**

****

****

****

| **Adresă IP** | **Locație** | **Porturi deschise** | **Servicii identificate** | **Sistem de operare** | **Alte observații** |
| --- | --- | --- | --- | --- | --- |
| 89.37.212.113  ROMARG HOSTING, RO | România | 25, 80, 143,443, 993, 2082, 2083, 2087, 2095, 2096 | SMTP,IMAP,IMAPS,  HTTP, HTTPS,  cPanel,WHM | Linux | - Folosit pentru multiple subdomenii olx.ro\n- Subnet: 89.37.212.0/24\n- ASN: 205275 |
| 136.147.129.27  SALESFORCE | United States | 25 | SMTP | Windows Server | Server de email |
| 5.134.209.128  GFL-POLAND, PL | Polonia | 80, 443 | HTTP, HTTPS | Nu este specificat | Posibil server intern |

## 1. Analiza per Server

### Server România (89.37.212.113)

* **Complexitate**: Ridicată (10 porturi deschise)
* **Funcționalitate**: Server multi-rol
* **Servicii critice**: Email, Web, Administrare
* **Expunere**: Majoră datorită varietății de servicii

### Server SUA (136.147.129.27)

* **Complexitate**: Scăzută (1 port deschis)
* **Funcționalitate**: Dedicat serviciului email
* **Servicii critice**: SMTP
* **Expunere**: Minimă, configurație specifică

### Server Polonia (5.134.209.128)

* **Complexitate**: Medie (2 porturi deschise)
* **Funcționalitate**: Server web
* **Servicii critice**: HTTP/HTTPS
* **Expunere**: Moderată, limitată la servicii web

## 2. Analiza de Risc

### Riscuri Majore Identificate

1. **Server România**:
   * Multiple servicii email necriptate (25, 143)
   * Interfețe administrative expuse (2082, 2083, 2087)
   * Servicii web pe porturi standard (80, 443)
2. **Server SUA**:
   * Port SMTP expus (potențial risc de spam/relay)
3. **Server Polonia**:
   * Configurație web standard (potential predictibilă)

### Vulnerabilități Potențiale

1. **Server România**:
   * Risc de interceptare email (porturi necriptate)
   * Atacuri de forță brută pe interfețele administrative
   * Cross-site scripting prin serviciile web
   * SQL injection prin aplicațiile web
2. **Server SUA**:
   * Email spoofing
   * SMTP relay attacks
   * Directory harvest attacks
3. **Server Polonia**:
   * Web application vulnerabilities
   * SSL/TLS misconfiguration
   * DDoS attacks

## 3. Recomandări de Securitate

### Imediate

1. Server România:
   * Dezactivarea porturilor email necriptate
   * Implementarea IP whitelisting pentru interfețele administrative
   * Configurarea WAF pentru serviciile web
2. Server SUA:
   * Implementarea filtrelor SMTP stricte
   * Configurarea SPF, DKIM și DMARC
3. Server Polonia:
   * Implementarea rate limiting
   * Configurarea security headers
   * Actualizarea certificatelor SSL/TLS

### Pe Termen Lung

* Implementarea unui sistem centralizat de logging
* Dezvoltarea unei politici de backup
* Planificarea auditurilor de securitate regulate
* Implementarea monitorizării continue

## Concluzie

Infrastructura prezintă o complexitate variată, cu serverul din România având cea mai mare suprafață de atac. Se recomandă o abordare stratificată a securității, cu accent pe reducerea expunerii serviciilor critice și implementarea controalelor de acces stricte.