

Relatório de Análise de Tráfego e Segurança

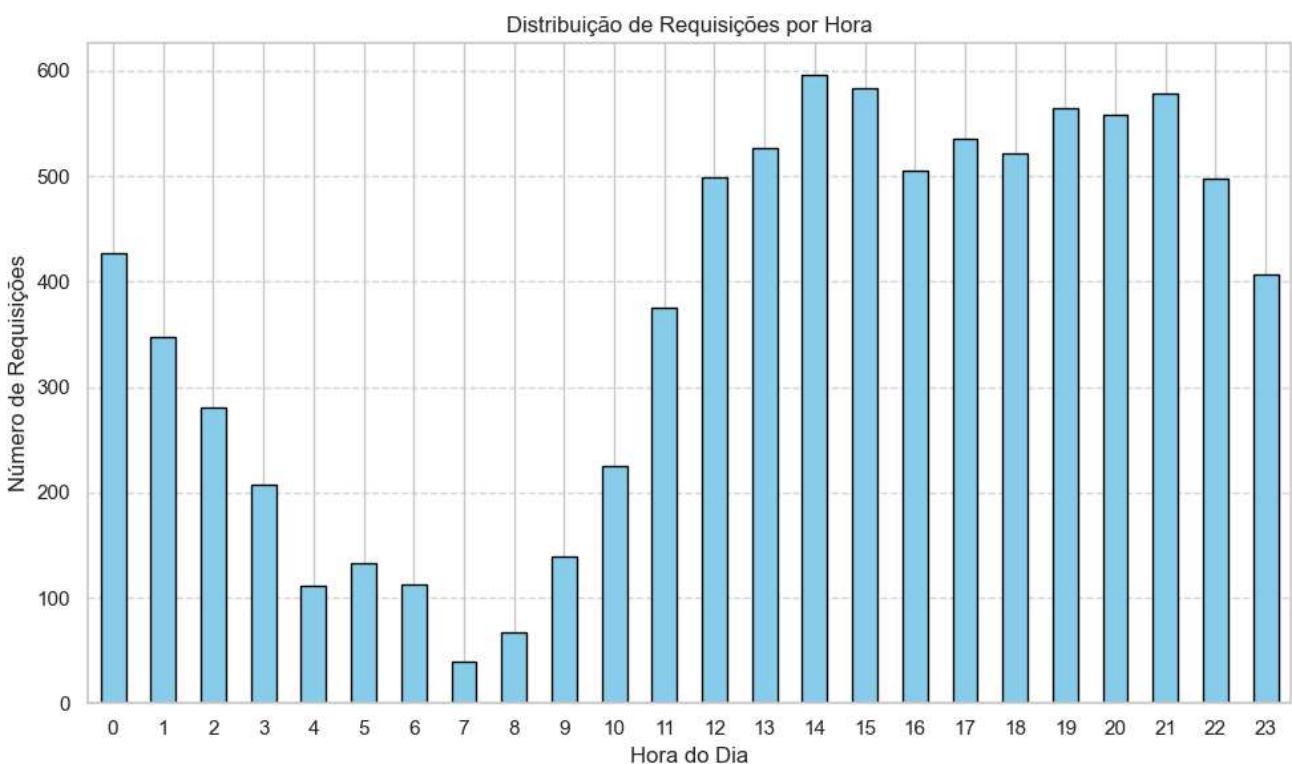
1. Introdução

Este relatório apresenta uma análise detalhada dos dados de tráfego coletados. O objetivo é identificar padrões de uso, riscos de segurança e propor soluções para mitigar vulnerabilidades detectadas.

2. Tráfego de Rede

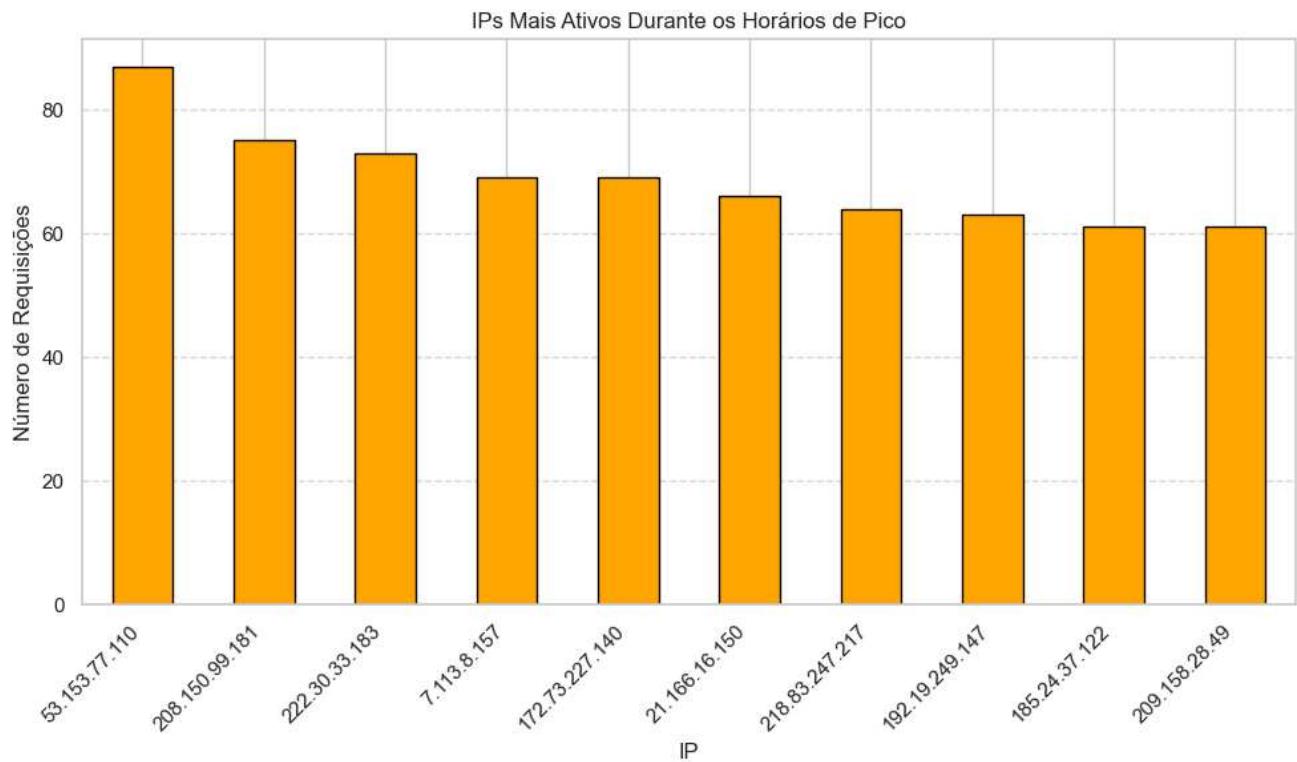
2.1 Distribuição de Requisições por Hora

Apresentação do gráfico que demonstra a distribuição do número de requisições ao longo das 24 horas do dia, destacando horários de maior atividade.



2.2 IPs Mais Ativos Durante os Horários de Pico

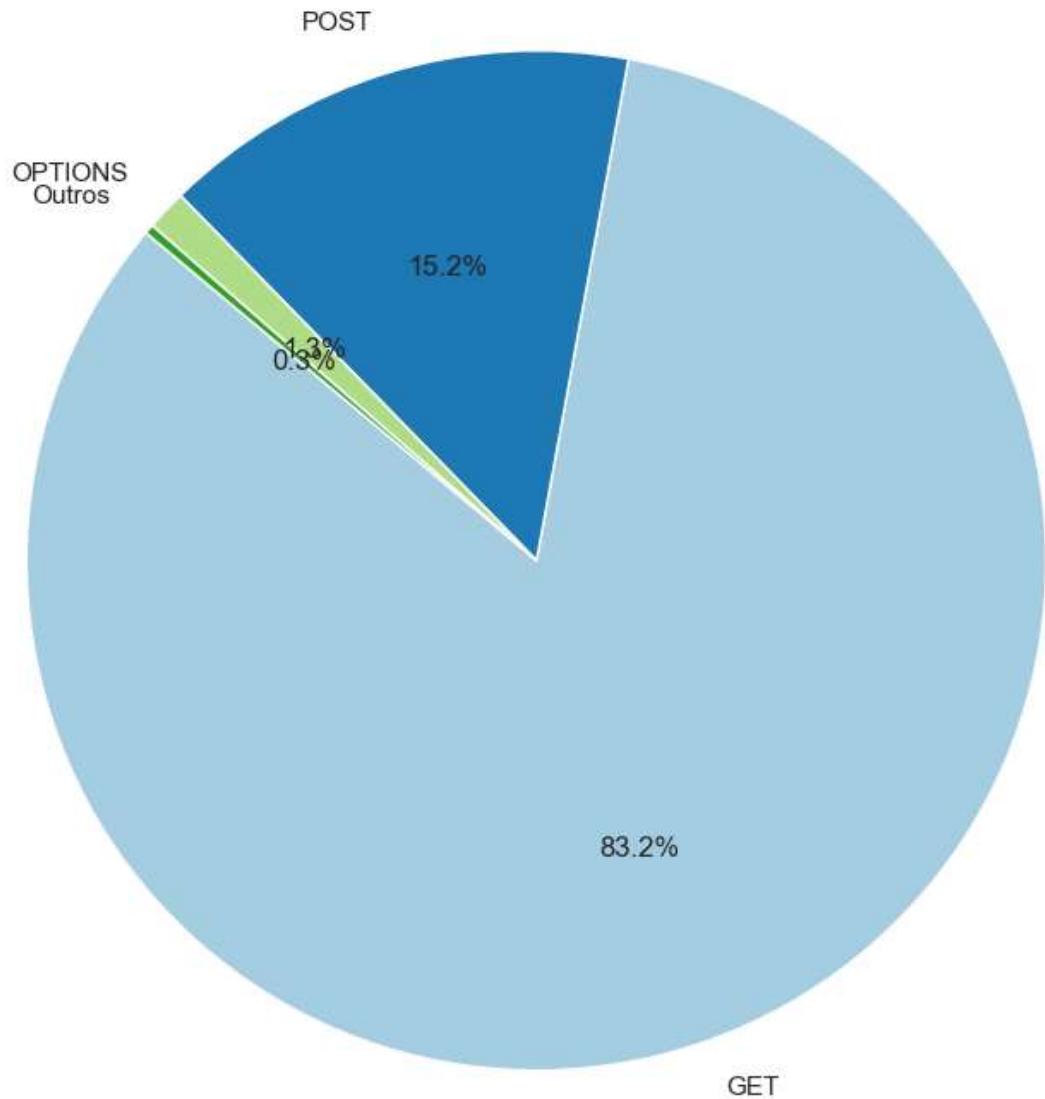
Análise dos IPs que mais realizaram requisições durante os horários de maior tráfego (13h às 21h). Gráfico de barras apresenta os 10 principais IPs.



2.3 Distribuição dos Métodos de Requisição

Descrição da distribuição de métodos HTTP utilizados (GET, POST, etc.) e seu percentual em relação ao total de requisições.

Distribuição dos Métodos de Requisição (Agrupado)



2.4 Distribuição Geográfica dos Acessos

A tabela demonstra a distribuição dos acessos por país, identificando regiões com maior concentração de tráfego.

| País (Sigla) | Número de Requisições |
|---------------------|------------------------------|
| 1 | India (in) 18372 |
| 2 | United States (us) 11481 |
| 3 | Brazil (br) 37 |
| 4 | Japan (jp) 34 |
| 5 | United Kingdom (gb) 26 |
| 6 | France (fr) 20 |
| 7 | China (cn) 10 |
| 8 | Germany (de) 8 |
| 9 | Australia (au) 8 |
| 10 | Canada (ca) 4 |

Recomendação: Avaliar se faz sentido permitir o acesso de outros países e se há necessidade de filtrar as requisições com base em geolocalização.

2.5 Contagem de IPs mais frequentes

Tabela apresentando os 20 IPs que mais realizaram requisições no ambiente. Essa análise é importante para identificar os principais emissores de tráfego, possibilitando diferenciar entre atividades legítimas e suspeitas, além de fornecer insights sobre comportamentos recorrentes no sistema.

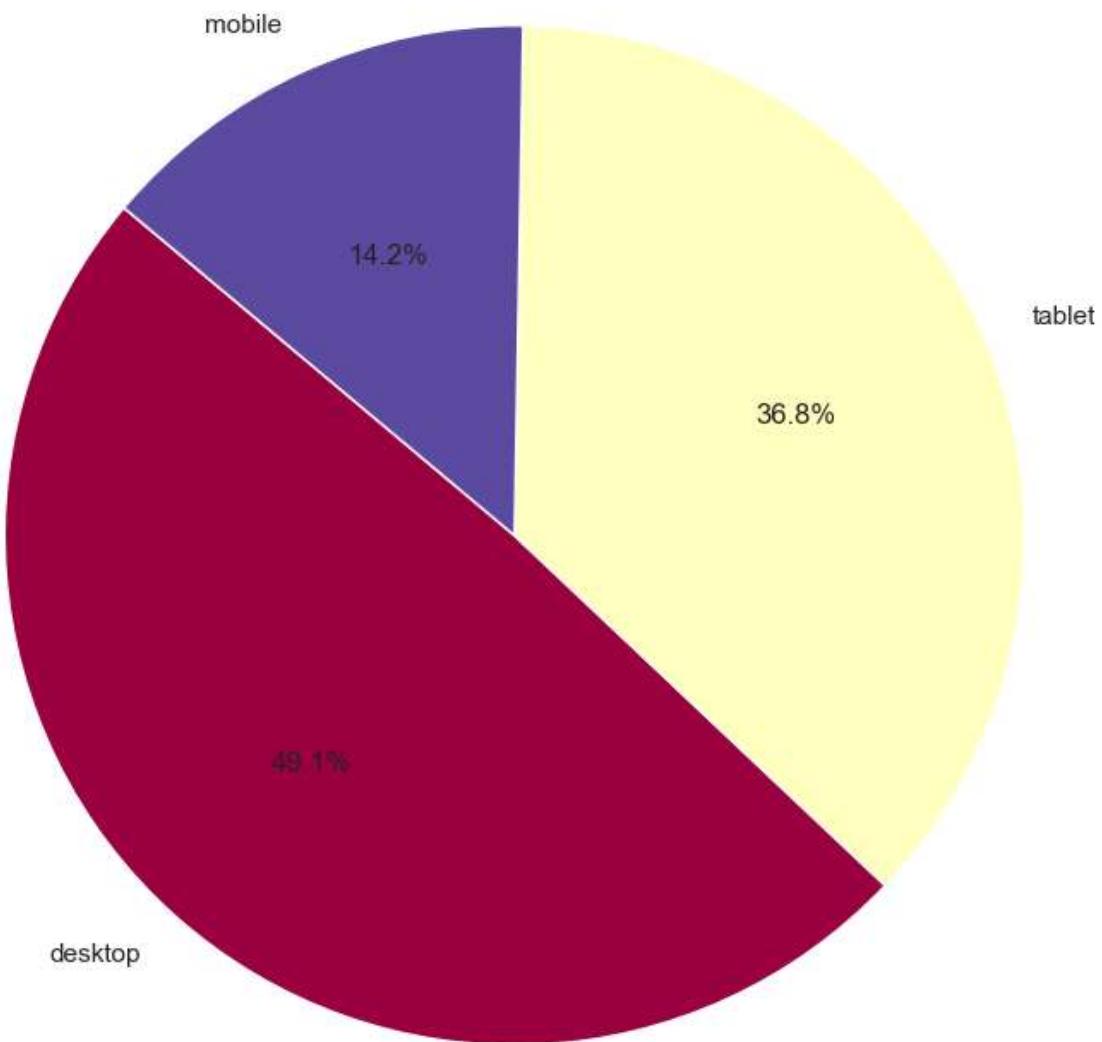
| IP | Número de Requisições |
|---------------------------|-----------------------|
| 1 53.153.77.110 | 156 |
| 2 208.150.99.181 | 119 |
| 3 125.227.246.131 | 116 |
| 4 185.24.37.122 | 115 |
| 5 209.158.28.49 | 114 |
| 6 129.53.13.62 | 114 |
| 7 222.30.33.183 | 114 |
| 8 159.168.200.38 | 112 |
| 9 21.166.16.150 | 112 |
| 10 192.19.249.147 | 112 |
| 11 195.171.155.166 | 110 |
| 12 11.148.137.128 | 109 |
| 13 157.226.241.234 | 108 |
| 14 13.235.167.220 | 107 |
| 15 88.40.53.243 | 106 |
| 16 26.158.117.152 | 106 |
| 17 56.172.84.231 | 105 |
| 18 117.200.193.5 | 105 |
| 19 132.107.158.218 | 105 |
| 20 172.73.227.140 | 105 |

Mais à frente será possível notar que os IPs com mais requisições também estão relacionados a requisições maliciosas, sendo recomendável o bloqueio, mesmo havendo tratamentos para evitar a exploração de vulnerabilidades.

2.5 Tipo de Dispositivo e Tráfego por Minuto

Análise do tráfego segregado por tipo de dispositivo (desktop, mobile, etc.) e gráfico mostrando os picos de tráfego por minuto. Identificação de picos anômalos de tráfego que podem indicar possíveis ataques ou atividades suspeitas.

Distribuição de Requisições por Tipo de Dispositivo (Spectral)



Média de tráfego por minuto: 2.84

Desvio padrão: 1.89

Límite para picos: 8.52

Picos de tráfego identificados:

EdgeStartTimestamp

2024-11-05 12:21:00+00:00 9

2024-11-05 13:11:00+00:00 10

2024-11-05 13:43:00+00:00 9

2024-11-05 14:03:00+00:00 9

2024-11-05 14:32:00+00:00 9

..

2024-11-14 14:20:00+00:00 11

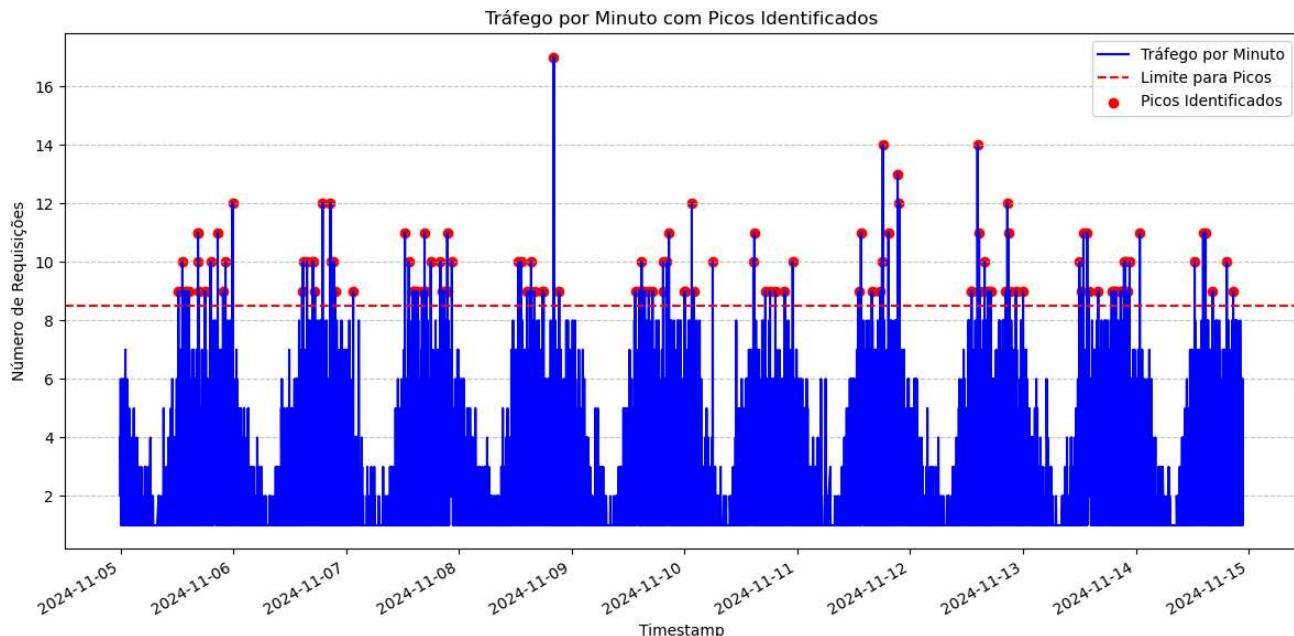
2024-11-14 14:51:00+00:00 11

2024-11-14 16:21:00+00:00 9

2024-11-14 19:21:00+00:00 10

2024-11-14 20:43:00+00:00 9

Name: count, Length: 126, dtype: int64



O monitoramento de tráfego acima do limite em uma aplicação é essencial para identificar e mitigar possíveis ameaças à segurança e desempenho da aplicação. Recomendação: Implementação de Rate Limits, restringindo o número de requisições que um usuário pode fazer num determinado período e usar redes de distribuição de conteúdo para reduzir o impacto nos servidores. É importante avaliar casos excepcionais como eventos promocionais em que o pico de acesso será atingido mas por usuários legítimos.

3. Identificação de Riscos de Segurança

3.1 Ocorrências de UserAgents

Contagem e análise dos UserAgents menos utilizados, o que pode sugerir tentativa de ataque utilizando ferramentas automatizadas ou scripts antigos para explorar vulnerabilidades conhecidas, bem como falsificar o User Agent para evitar detecção ou enganar sistemas de segurança.

UserAgents Incomuns (menos de 5 ocorrências):

| Nº | UserAgent | Número de Ocorrências |
|------|--|-----------------------|
| 1 | Mozilla/5.0 (Windows; U; Windows NT 6.2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.6045.102 Safari/537.36 | 4 |
| 2 | Mozilla/5.0 (Android 2.2.2; Mobile; rv:46.0) Gecko/20100101 Firefox/46.0 | 4 |
| 3 | Opera/8.22.(Windows NT 5.1; az-AZ) Presto/2.9.15 Version/11.00 | 4 |
| 4 | Mozilla/5.0 (Macintosh; U; PPC Mac OS X 10_8_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.6045.102 Safari/537.36 | 4 |
| 5 | Opera/8.95.(Windows 98; is-IS) Presto/2.9.179 Version/11.00 | 4 |
| ... | ... | ... |
| 2377 | Opera/9.35.(X11; Linux x86_64; crh-UA) Presto/11.00 | 1 |
| 2378 | Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_15_7; en-US) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.6045.102 Safari/537.36 | 1 |
| 2379 | Mozilla/5.0 (Android 2.0; Mobile; rv:55.0) Gecko/20100101 Firefox/55.0 | 1 |
| 2380 | Mozilla/5.0 (Windows; U; Windows CE) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.6045.102 Safari/537.36 | 1 |
| 2381 | Mozilla/5.0 (iPod; U; CPU iPhone OS 3_3 like Mac OS X; en-US) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.6045.102 Safari/537.36 | 1 |

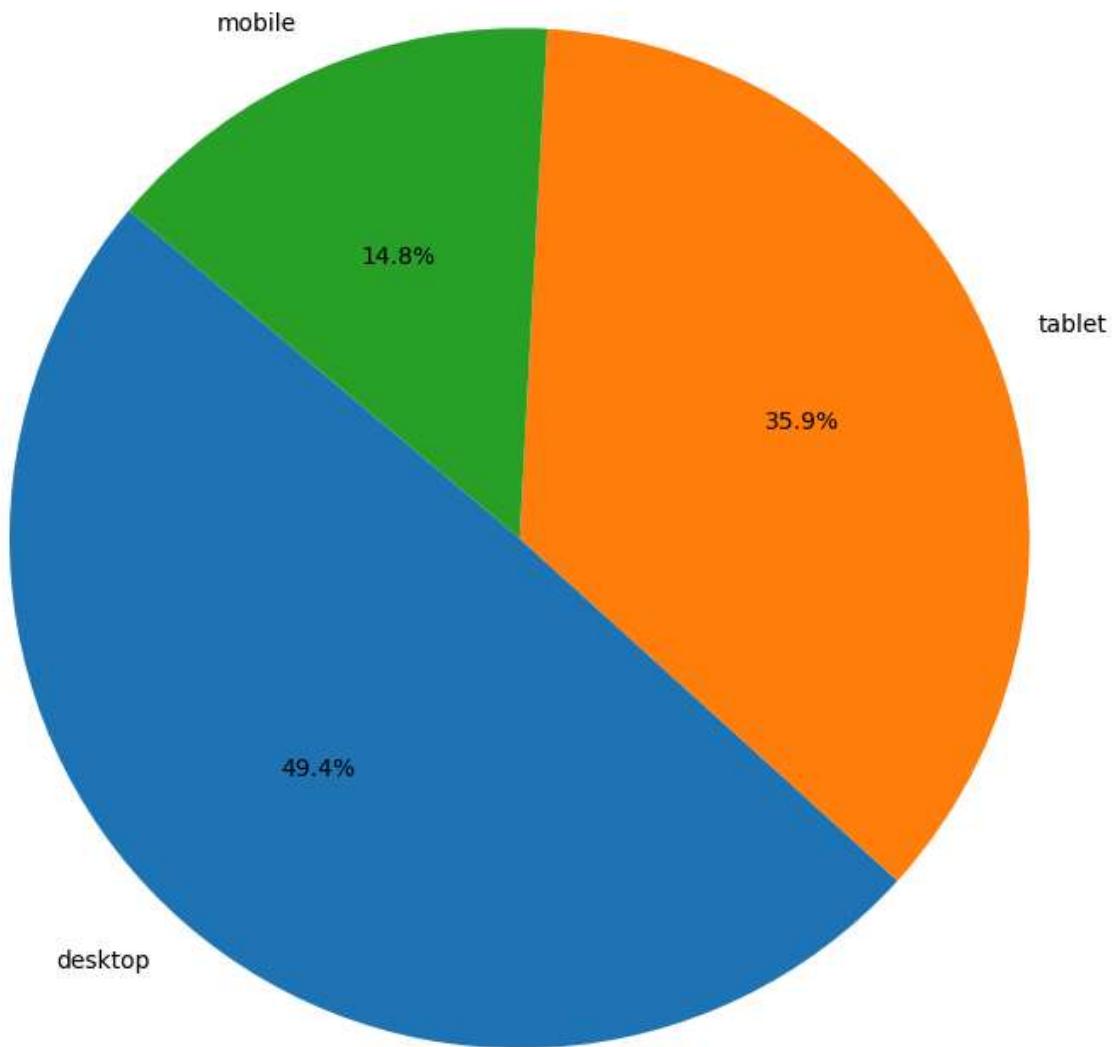
[2381 rows x 2 columns]

Recomendação: Criar uma lista de User Agents permitidos para acesso à aplicação e bloqueie de User Agents que não atendam a critérios predefinidos(antigos, desatualizados, sistemas legados, etc.).

3.2 Distribuição de Injeções por Tipo de Dispositivo

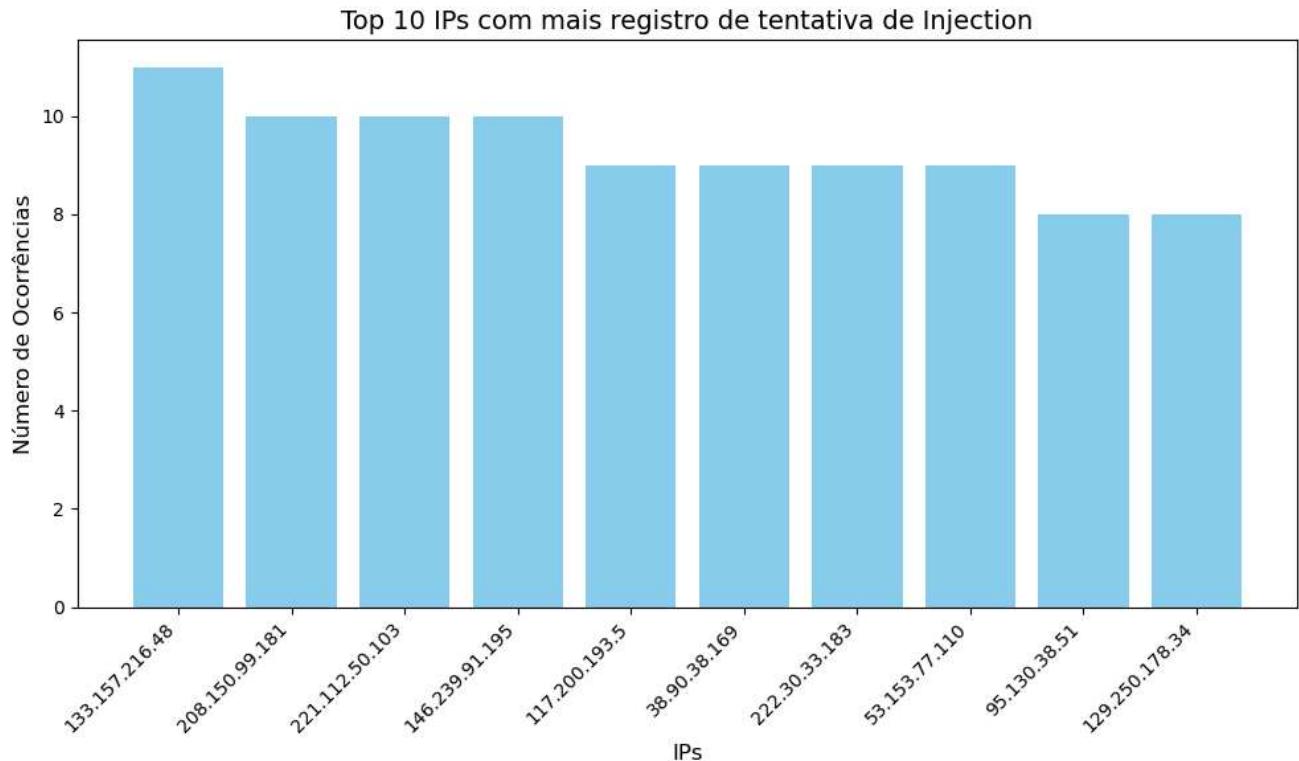
Análise da distribuição de tentativas de exploração de vulnerabilidades do tipo Injection, com base no tipo de dispositivo utilizado.

Distribuição de Injection por Tipo de Dispositivo (ClientDeviceType)



3.3 Distribuição de Injeções por IP, classificado em TOP 10

Análise da distribuição de tentativas de exploração de vulnerabilidades do tipo Injection, separado por número de tentativas por IP.



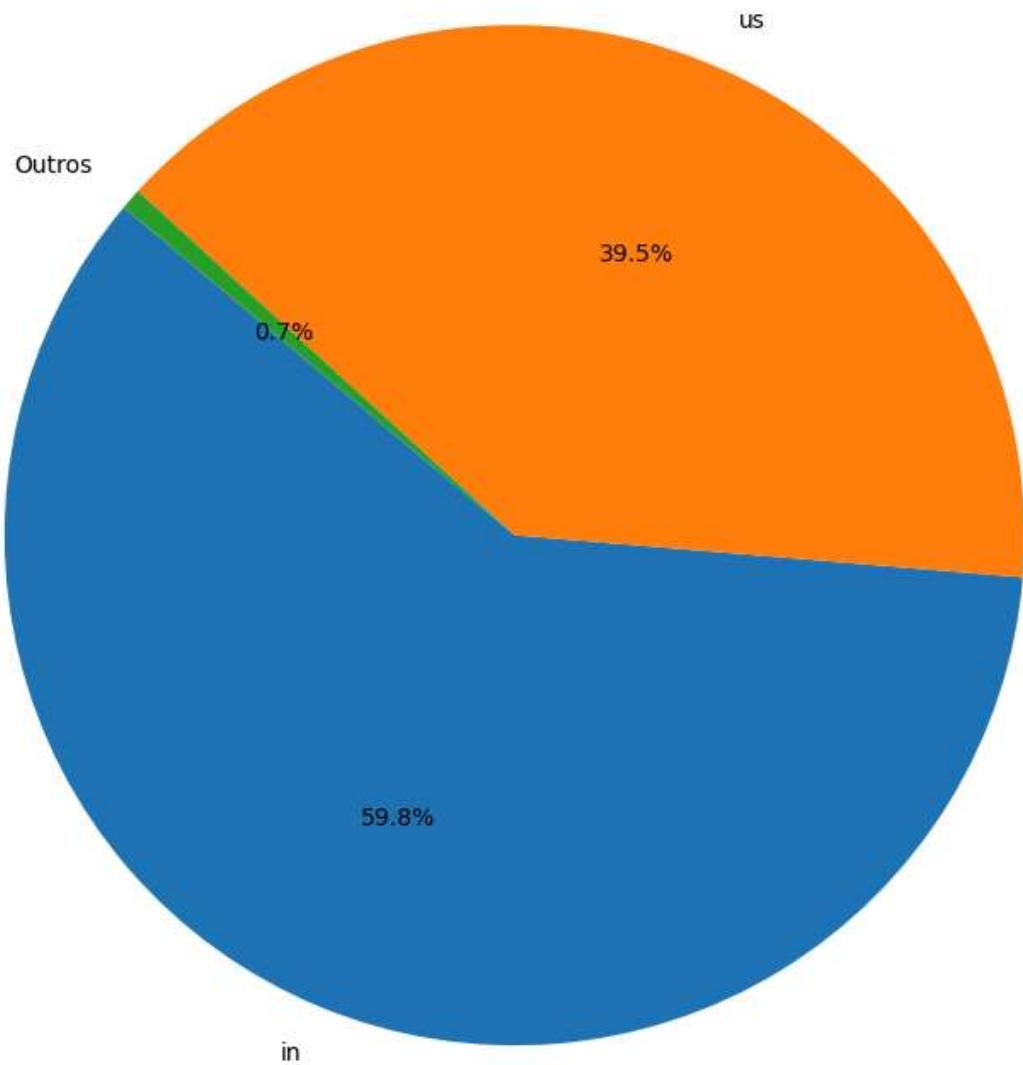
Ips com muitas requisições também estão associados à tentativa de exploração de vulnerabilidades do tipo Injection, alguns dez recorrências ou mais.

Recomendação: Bloquear os IPs maliciosos, validar todas as entradas para que não aceitem quaisquer caracteres e use prepared statements no banco de dados. Se aplicável, utilizar um firewall de aplicação que bloqueia este tipo de requisição em tempo real e também utilize bibliotecas anti-XSS.

3.3 Distribuição de Injeções por País

Classificação das tentativas de injeção por origem geográfica (top 2 países mais frequentes + outros).

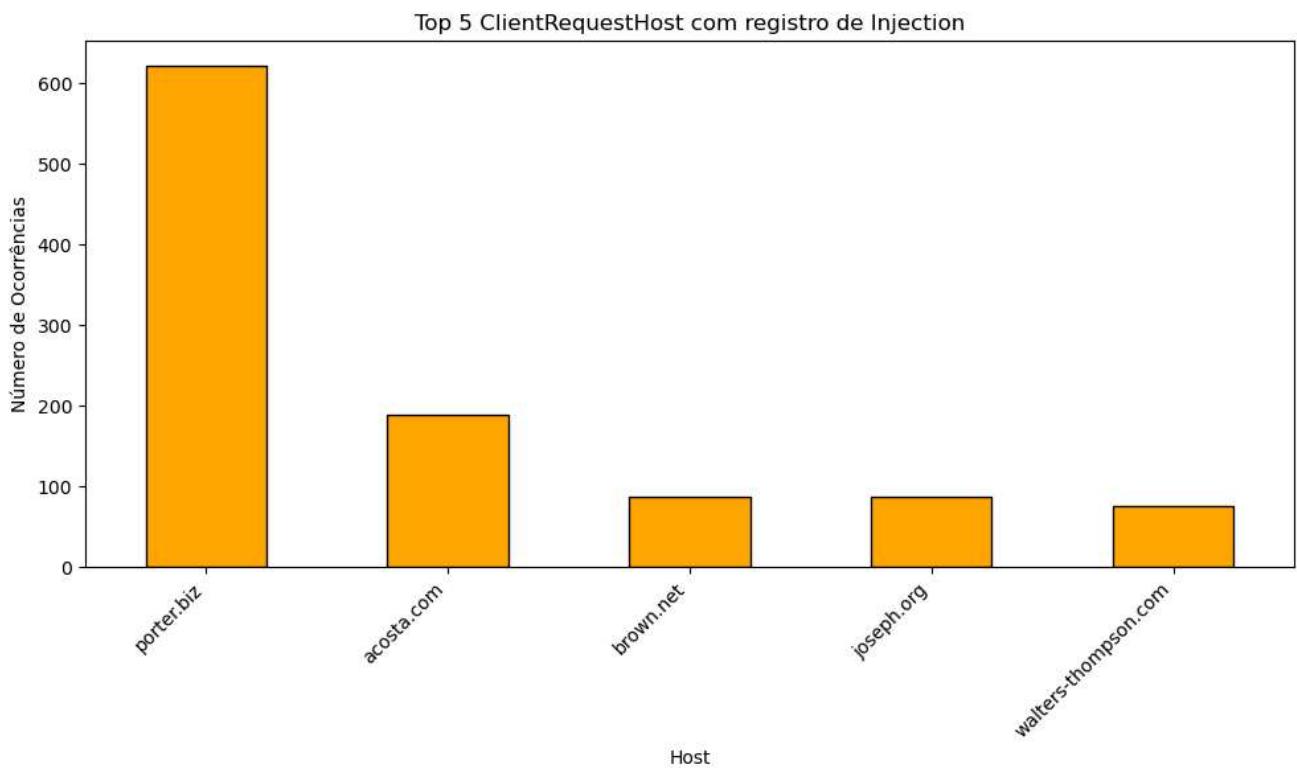
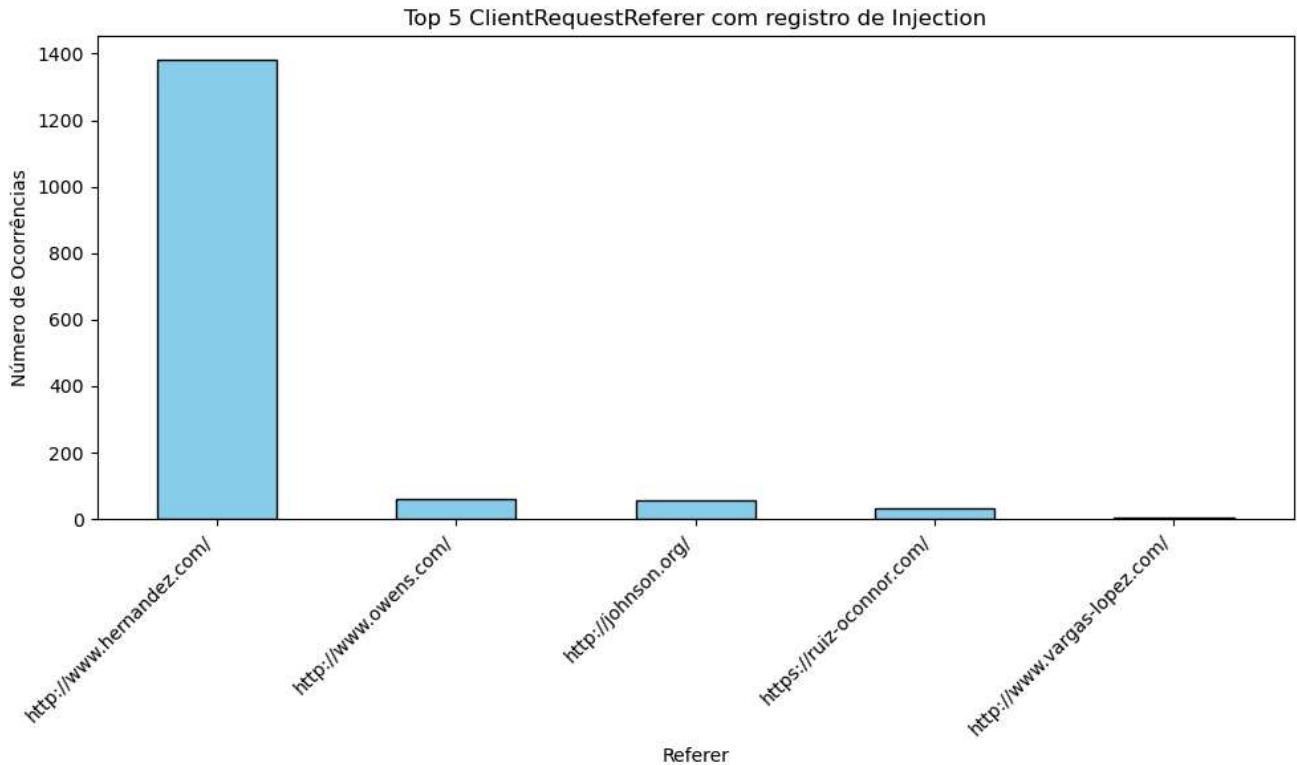
Distribuição de Injection por País (Top 2 + Outros)



Recomendação: Validar se faz sentido a aplicação receber acesso de determinados países e criar regras de bloqueio por geolocalização para evitar ocorrência de acessos indevidos. Melhora a segurança da aplicação e sua performance, uma vez que esses acessos deixam de consumir recursos.

3.5 Referers e Hosts Relacionados a Injeções

A identificação de referers e hosts relacionados a tentativas de injeção é crucial para entender a origem dos ataques, o comportamento dos atacantes e mitigar futuras tentativas. Identificação dos principais referers e hosts que registraram tentativas de injeção (top 5).



Recomendação: Identificar se os referers são de sites legítimos. Aplicar regras de rate limit por Host e Referer, limitando a frequência de requisições vindas de aplicações suspeitas.

3.6 Resumo do Tráfego de IPs Associados a Vulnerabilidades

Descrição do comportamento dos IPs identificados como associados a exploração de vulnerabilidades, incluindo volume de requisições e bytes trafegados. É possível notar que alguns IPs registrados com

Resumo do Tráfego de Ips que realizaram alguma exploração de Vulnerabilidade:

IP mais ativo: 53.153.77.110

- Total de requisições: 156

- Total de bytes trafegados: 713,109

Tráfego geral:

- Total de requisições de Ips Maliciosos: 8835

- Total de bytes trafegados de Ips Maliciosos: 58,800,686

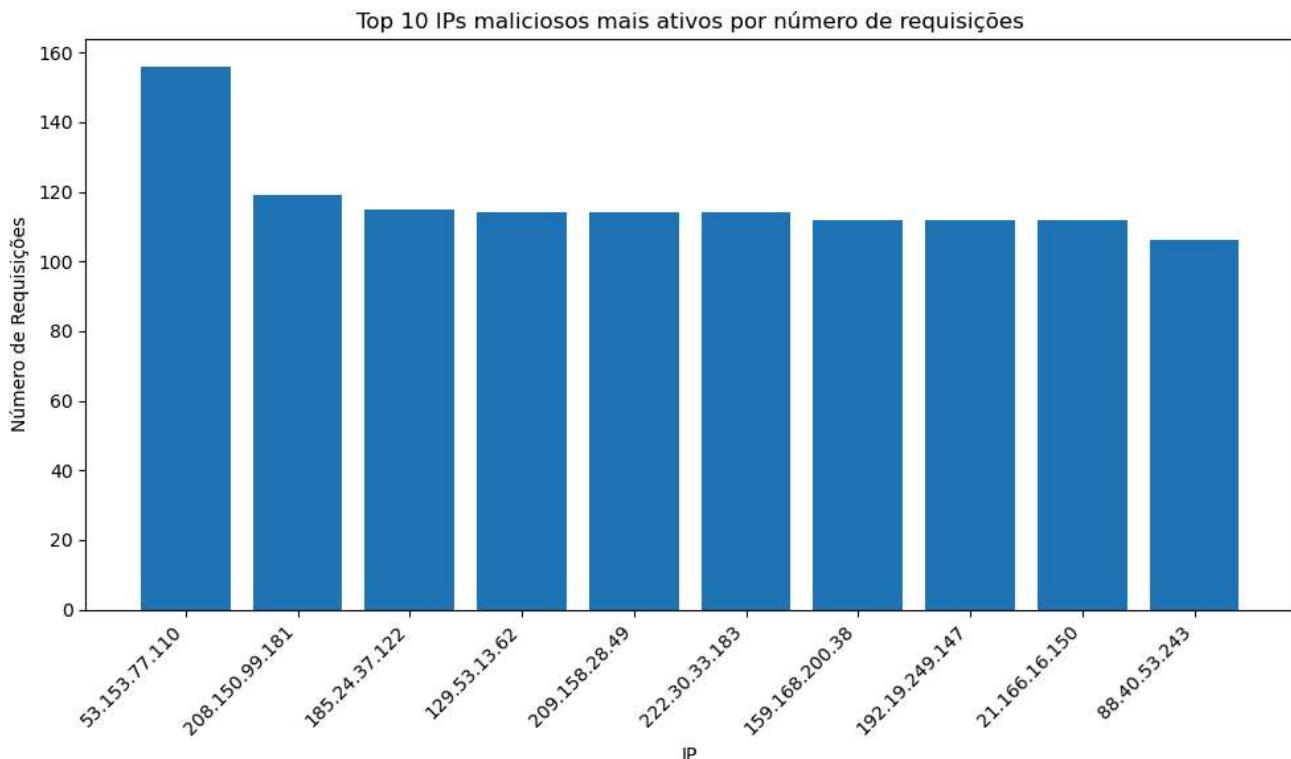
Top 10 IPs maliciosos mais ativos:

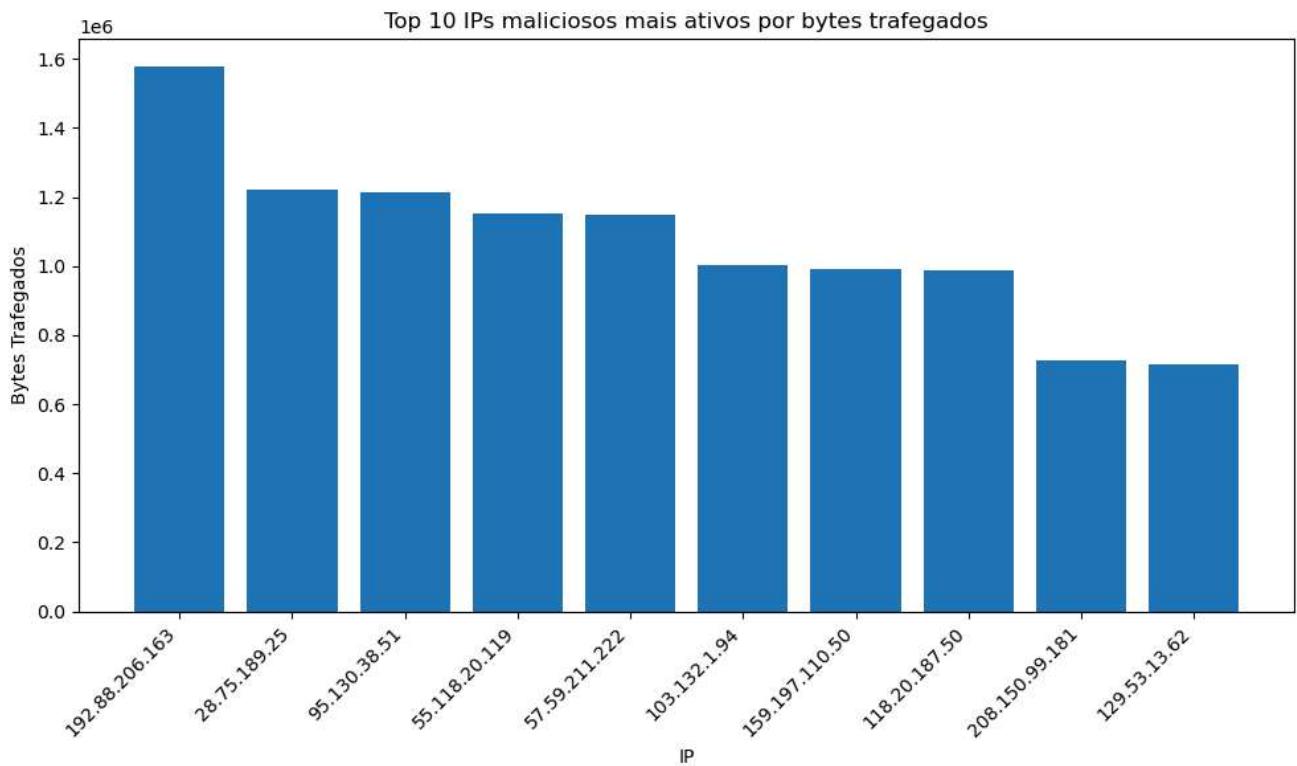
| | ClientIP | total_requests | total_bytes |
|-----|----------------|----------------|-------------|
| 568 | 53.153.77.110 | 156 | 713109 |
| 348 | 208.150.99.181 | 119 | 725866 |
| 262 | 185.24.37.122 | 115 | 713783 |
| 405 | 222.30.33.183 | 114 | 713018 |
| 352 | 209.158.28.49 | 114 | 706929 |
| 96 | 129.53.13.62 | 114 | 716627 |
| 182 | 159.168.200.38 | 112 | 675535 |
| 357 | 21.166.16.150 | 112 | 680727 |
| 285 | 192.19.249.147 | 112 | 676866 |
| 764 | 88.40.53.243 | 106 | 643736 |

Aplicar filtros e regras de bloqueio em IPs com comportamento malicioso mantém a aplicação mais segura e melhora a performance. Das 30 mil linhas da tabela, 8 mil estão associadas a Ips que realizaram alguma tentativa de exploração de vulnerabilidade, isso representa 58,800,686 bytes que não deveriam ter sido trafegados, ou consumidos pela aplicação.

3.7 Top 10 IPs Maliciosos

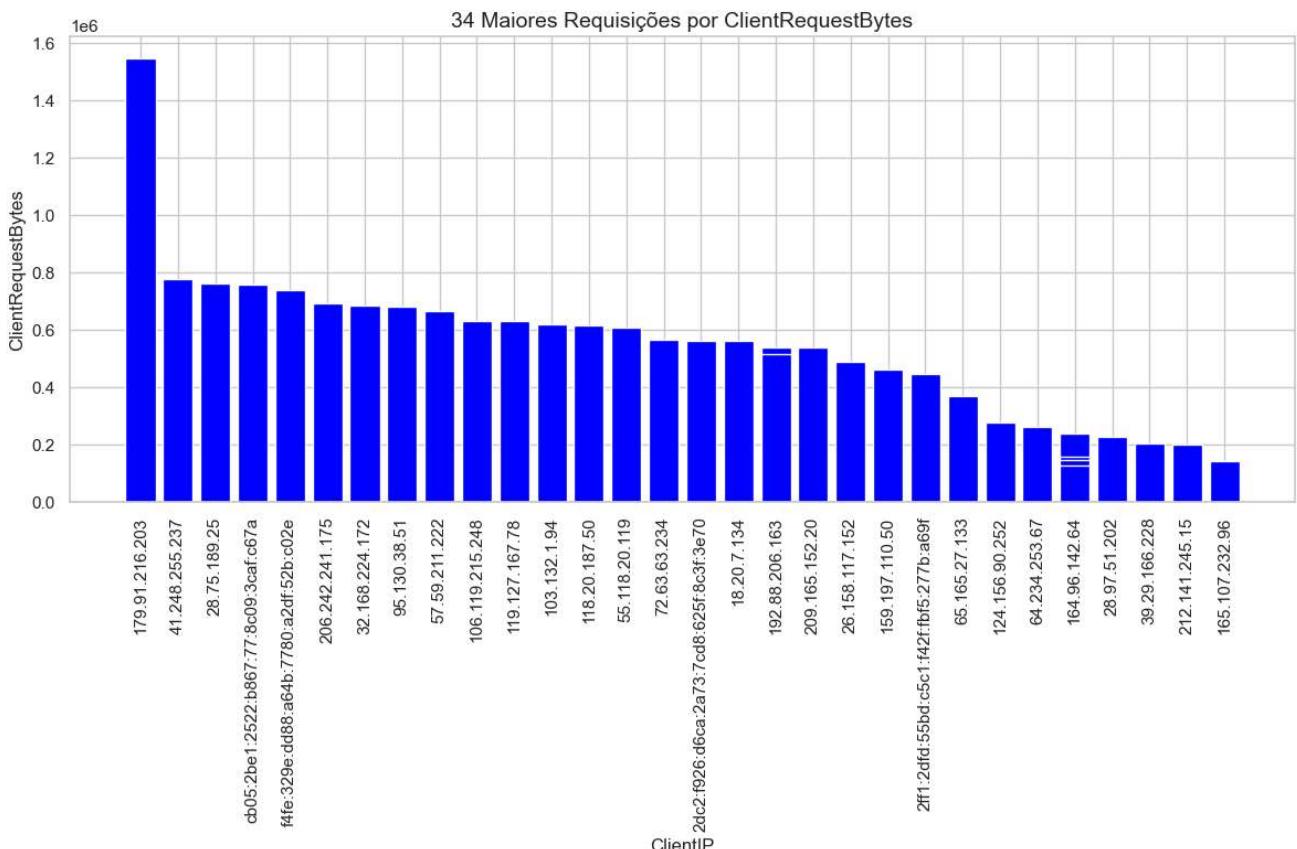
Listagem dos 10 IPs mais ativos relacionados a atividades maliciosas, considerando volume de requisições e dados trafegados.





4. Requisições excessivamente grandes

Requisições excessivamente grandes podem indicar possíveis ataques DDoS, abusos de recursos, ou erros de configuração.



Recomendação: Verificar se os IPs que realizaram essas requisições são confiáveis, bloquear IPs suspeitos através do WAF ou sistemas de gerenciamento de tráfego, confirmar se há endpoints que permitem transferências muito grandes ou desnecessárias e ajustar a lógica de negócios para limitar os dados retornados

5. Conclusão

A análise apresentada foi realizada utilizando Python como linguagem principal, em conjunto com o Jupyter Notebook como ferramenta para processamento e visualização dos dados. Com base nos dados fornecidos, identificou-se que quase 1/3 das requisições analisadas possuem origem maliciosa, destacando a importância de medidas proativas de segurança.

Além disso, há uma parcela significativa de requisições que necessitam de dados complementares para determinação precisa da intenção, indicando a necessidade de monitoramento contínuo e coleta de informações adicionais.

Apesar da gravidade das descobertas, as medidas preventivas para mitigar os riscos são relativamente simples e de fácil implementação, incluindo:

- Validação de entradas para prevenir injeções;
- Configuração de firewalls para bloquear IPs maliciosos;
- Uso de ferramentas como WAFs para proteção em tempo real;
- Monitoramento contínuo para detecção de padrões anômalos;

Essas ações, se implementadas adequadamente, podem reduzir drasticamente a superfície de ataque e proteger a aplicação contra tentativas maliciosas.

Anexos: Gráficos, tabelas e logs detalhados que suportam as análises apresentadas.