CPTarget

Analise de Fraude e Duplicidade de Leads

Campanha O Boticario - IR (Inicio de Revenda)

Periodo: Setembro/2025 - Abril/2026

Data: 09 de Abril de 2026

1. Resumo Executivo

Foram analisados 5942 leads contendo 3817 IPs unicos, coletados entre setembro/2025 e abril/2026. A analise utilizou Kali Linux com Nmap, WHOIS, DNS, ip-api.com, blacklists e scoring temporal.

Metrica	Valor
Total de Leads	5942
IPs Unicos	3817
Leads Duplicados	2684 (45.2%)
Leads Fantasma (sem IP)	517 (8.7%)
% Conexoes Mobile	100.0%

2. Metodologia

Ambiente: Homelab 192.168.0.5 (Debian 13, Docker v29.3.0). Container Kali Linux (infra_kali).

Ferramenta	Funcao	Escopo
ip-api.com (batch)	Geo, ISP, tipo conexao, proxy/VPN	3.817 IPs (100%)
whois	Owner, CNPJ, abuse contact, CIDR	2.464 IPs (64.6%)
dig -x	Reverse DNS	3.768 IPs (98.7%)
nmap -sV -O	OS fingerprint, portas, banners	100 IPs (top)
nmap dns-blacklist	Listas negras DNS	200 IPs (top)
traceroute	Rota de rede, hops	30 IPs (amostra)
TOR bulk exit list	Exit nodes TOR	3.817 IPs (100%)
Python (analise)	Scoring temporal, clustering	3.817 IPs (100%)

3. Cobertura do Enriquecimento

Camada	Coletados	Cobertura
Geolocalizacao	3817	100%
Classificacao + Subnet Density	3.817	100%
Reverse DNS	3768	98.7%
WHOIS completo	2464	64.6%
Temporal scoring	1076	100% duplicados
TOR exit check	3.817	100%
Nmap OS + Banner	100	Top IPs
DNS Blacklist	200	Top IPs
Traceroute	30	Amostra

4. Classificacao dos IPs

100% dos IPs sao de rede celular brasileira (CGNAT). Nenhum datacenter, proxy, VPN ou TOR.

Classe	IPs	%
mobile_tim (TIM Celular - CGNAT)	3.794	99.4%
mobile_vivo (Telefonica/Vivo)	23	0.6%

5. Flags de Risco

Flag	IPs	Leads
ALTO	4	14
MEDIO	159	607
BAIXO	913	2063
OK	2741	2741

6. Deteccao de Anomalias

Anomalia	Resultado	Significado
Score bot >= 0.5	26 IPs	Alta suspeita automacao
Score bot >= 0.3	39 IPs	Media suspeita
Padrao temporal regular	30 IPs	Intervalos constantes
Leads mesmo dia (2+)	62 IPs	Multiplos cadastros/dia
Vizinhos sequenciais	2161 IPs	IP adjacente no dataset
Proxy / VPN / TOR / Blacklist	0	Nenhum detectado

7. Top 15 IPs - Score de Bot

IP	Score	Leads	Max/Dia	Analise
189.40.88.231	0.90	3	3	Todos no mesmo dia
189.40.90.88	0.90	3	3	Todos no mesmo dia
189.40.75.121	0.60	2	2	Todos no mesmo dia
189.40.72.100	0.60	2	2	Todos no mesmo dia
189.40.73.87	0.60	2	2	Todos no mesmo dia
189.40.73.72	0.60	2	2	Todos no mesmo dia
177.50.36.105	0.60	2	2	Todos no mesmo dia
177.30.135.3	0.60	2	2	Todos no mesmo dia
177.30.151.64	0.60	2	2	Todos no mesmo dia
177.50.36.85	0.60	2	2	Todos no mesmo dia
177.50.13.236	0.60	2	2	Todos no mesmo dia
189.40.72.87	0.60	2	2	Todos no mesmo dia
177.30.132.178	0.60	2	2	Todos no mesmo dia
189.40.72.140	0.60	2	2	Todos no mesmo dia
189.40.74.113	0.60	2	2	Todos no mesmo dia

8. Top 30 IPs Duplicados

IP	Leads	Risco	Max/Dia	Provedor	Cidade	De	Ate
189.40.72.60	6	MEDIO	1	-	São Paulo	2026-01-29	2026-03-19
189.40.73.15	6	MEDIO	1	-	São Paulo	2026-01-29	2026-03-25
189.40.72.70	6	MEDIO	1	-	São Paulo	2026-02-03	2026-04-06
189.40.73.63	6	MEDIO	1	-	São Paulo	2026-01-29	2026-04-02
189.40.88.75	6	MEDIO	1	TIM CELULAR S.A.	São Paulo	2026-02-02	2026-04-06
189.40.89.82	6	MEDIO	1	TIM CELULAR S.A.	São Paulo	2026-01-20	2026-03-05
189.40.89.174	5	MEDIO	1	TIM CELULAR S.A.	São Paulo	2026-02-06	2026-04-03
189.40.90.167	5	MEDIO	1	TIM CELULAR S.A.	São Paulo	2026-02-10	2026-04-02
189.40.75.89	5	MEDIO	1	-	São Paulo	2026-02-13	2026-04-07
189.40.72.44	5	MEDIO	1	-	São Paulo	2026-02-10	2026-03-30
189.40.74.106	5	MEDIO	1	-	São Paulo	2026-02-03	2026-03-19
189.40.89.232	5	MEDIO	1	TIM CELULAR S.A.	São Paulo	2026-01-31	2026-04-02
189.40.91.180	5	MEDIO	1	TIM CELULAR S.A.	São Paulo	2026-02-12	2026-03-16
189.40.75.222	5	MEDIO	1	-	São Paulo	2026-02-21	2026-03-27
189.40.75.195	5	MEDIO	2	-	São Paulo	2026-01-14	2026-03-23
189.40.91.251	5	MEDIO	1	TIM CELULAR S.A.	São Paulo	2026-02-10	2026-04-03
189.40.89.94	5	MEDIO	1	TIM CELULAR S.A.	São Paulo	2026-01-12	2026-03-14
189.40.73.104	5	MEDIO	2	-	São Paulo	2026-01-14	2026-03-24
189.40.74.16	5	MEDIO	2	-	São Paulo	2026-02-28	2026-04-06
189.40.89.99	5	MEDIO	1	TIM CELULAR S.A.	São Paulo	2026-02-03	2026-03-31
189.40.88.36	5	MEDIO	1	TIM CELULAR S.A.	São Paulo	2026-02-17	2026-03-25
189.40.91.179	5	MEDIO	2	TIM CELULAR S.A.	São Paulo	2026-02-20	2026-03-24
189.40.73.144	5	MEDIO	2	-	São Paulo	2026-02-09	2026-04-03
189.40.90.118	5	MEDIO	1	TIM CELULAR S.A.	São Paulo	2026-02-17	2026-03-27
189.40.89.194	5	MEDIO	1	TIM CELULAR S.A.	São Paulo	2026-01-21	2026-04-06
189.40.75.249	5	MEDIO	1	-	São Paulo	2026-02-11	2026-03-27
189.40.75.235	5	MEDIO	2	-	São Paulo	2026-02-17	2026-04-02
189.40.73.12	4	MEDIO	1	-	São Paulo	2026-02-05	2026-04-02
189.40.72.252	4	MEDIO	2	-	São Paulo	2026-02-10	2026-04-06
189.40.89.124	4	MEDIO	1	TIM CELULAR S.A.	São Paulo	2026-01-09	2026-03-21

9. Provedores e Geolocalizacao

Provedor (WHOIS)	IPs

Cidade - Estado	IPs
São Paulo - São Paulo	3794
Campinas - São Paulo	23

10. Densidade de Subnet (Top 10 /24)

Bloco /24	IPs	Leads

11. Analise por Campanha

Campanha	Leads	IPs	Dup	S/IP	%Dup
oboticario_interno_alwayson_ir_conversao_cpta	2832	2250	1353	108	47.8
oboticario_interno_alwayson_ir_conversao_cpta	2705	2218	1320	26	48.8
oboticario-interno-alwayson-ir-conversao-cpta	189	0	0	189	0.0
oboticario-interno-alwayson-ir-conversao-cpta	113	0	0	113	0.0
oboticario_interno_alwayson_ir_conversao_cpta	61	0	0	61	0.0
oboticario_interno_alwayson_ir_conversao_cpta	36	22	11	14	30.6

oboticario_interno_alwayson_ir_conversao_cpta	6	0	0	6	0.0

12. Conclusoes e Recomendacoes

CONCLUSOES:

1. Concentracao extrema: 99.4% dos leads vem da TIM (AS26615), todos CGNAT mobile. Deduplicacao por IP e ineficaz neste cenario.

2. Duplicidade significativa: 2.684 leads (45.2%) de IPs repetidos. 26 IPs com score bot >= 0.5.

3. Leads fantasma: 517 (8.7%) sem IP/origem/transaction_id - impossivel auditar.

4. Sem ameacas externas: Zero proxy, VPN, TOR, datacenter ou blacklisted. Fraude, se existente, e via dispositivos moveis reais.

5. Geo concentrada: 99.4% Sao Paulo-SP.

RECOMENDACOES:

1. Implementar device fingerprinting (canvas, user agent, screen) alem do IP.

2. Adicionar captcha nos formularios de cadastro.

3. Monitorar leads sem transaction_id (6.6% do total).

4. Deduplicar por IP+dia (mesmo IP no mesmo dia = lead unico).

5. Diversificar fontes de trafego (93% vem de uma unica origem).

6. Investigar manualmente os 26 IPs com score bot >= 0.5.

Gerado pelo sistema CPTarget Analysis | Kali Linux + PostgreSQL 17 + Python 3

Homelab 192.168.0.5 | Proxmox LXC / Docker v29.3.0