Relatório de Threat Intelligence – IP **1.1.1.1**

> **Fonte dos dados**: WHOIS (Sysinternals), Urlscan.io, VirusTotal API v3, AlienVault OTX, Netlas, cURL (Análise de Cabeçalhos HTTP), IPInfo.io, AbuseIPDB, Scamalytics, VPNAPI.
> **Timestamp da Análise**: 2026-02-14T13:54:20.890239.

1. Resumo Executivo

O IP 1.1.1.1 é um endereço Anycast de infraestrutura pública legítima, operado pela **Cloudflare, Inc. (AS13335)** em parceria com a APNIC, servindo principalmente como um resolvedor de DNS público (1.1.1.1). Geograficamente, é registrado na Austrália, mas sua natureza Anycast significa que o tráfego é roteado para o datacenter mais próximo. A reputação do IP é majoritariamente positiva, com pontuação de risco baixo ou neutro na maioria das ferramentas e sem detecções maliciosas ativas. No entanto, análises de superfície revelam que este IP é **amplamente utilizado por atores de ameaças como parte de sua infraestrutura de ofuscação**, servindo como ponto de contato para redirecionamentos maliciosos, hospedando páginas de bloqueio (403) para domínios de phishing e sendo sinalizado como VPN/Proxy. Portas críticas abertas incluem 53/UDP/TCP (DNS), 80/TCP (HTTP) e 443/TCP (HTTPS).

2. Análise de Comportamento

Fonte	Evidência	Interpretação
VirusTotal	Score de reputação 78, **0/93 detecções maliciosas**. 40 votos maliciosos de usuários.	Reputação técnica limpa, sem detecções ativas por motores de antivírus. Os votos de usuários indicam percepção negativa ou associação a incidentes indiretos.
AlienVault OTX	Reputação neutra (score 0). **Listado como falso positivo conhecido e em prefixo whitelist**. Nenhum pulso de ameaça ativo associado.	A plataforma reconhece oficialmente que o IP é legítimo e que aparições em contextos de ameaça são geralmente falsos positivos.
Urlscan.io	IP identificado como **servidor de bloqueio (403 Forbidden)** para **inúmeros domínios maliciosos** (ex: `xyzverse.site`, `admin.cukrarnavanilka.cz`). Tags incluem "phishdestroy", "phishing", "redirecionamento suspeito".	Evidência concreta de que atores maliciosos estão **configurando seus domínios para apontar para 1.1.1.1**, usando a infraestrutura confiável da Cloudflare para ocultar servidores reais ou servir páginas de erro, um padrão comum em campanhas de phishing e fraudes.
AbuseIPDB	**Score de abuso 0 (whitelisted)**, porém com **392 relatórios históricos de 58 usuários distintos**. Último reporte com data anômala (2026-02-14).	O alto volume de relatórios sugere **abuso indireto constante**, possivelmente relacionado a ataques de reflexão DNS ou uso do IP como destino em scripts maliciosos. A data futura indica possível inconsistência nos dados.

Fonte	Evidência	Interpretação
Netlas	Associado a **44.295 domínios**, incluindo vários com nomenclaturas suspeitas (ex: `168168168168168.vip`, `12138000.xyz`).	O volume massivo de domínios, muitos com padrões anômalos, reforça que o IP é um **ponto focal para tráfego diversificado**, parte do qual é claramente malicioso, abusando da reputação limpa da infraestrutura.
VPNAPI	Sinalizado como **VPN e Proxy**. Ausência de dados geolocalizáveis precisos.	Indica que o IP possui características que permitem **ocultação de tráfego**, sendo usado para ofuscar a origem real das conexões, um padrão valioso para ataques.
cURL / Shodan (implícito)	Redirecionamento 301 para HTTPS, cabeçalhos padrão da Cloudflare (`CF-RAY`), serviço de DNS respondendo.	Comportamento técnico esperado e legítimo para o serviço 1.1.1.1. Não indica comprometimento direto do próprio IP.
Scamalytics	Risco de frade **baixo (score 0)**. Identificado como tráfego de datacenter. Não está em blacklists.	Confirma a natureza legítima do IP como infraestrutura de rede, não sendo um host de usuário final comprometido.

Conclusão: O IP **1.1.1.1** é, em sua operação principal, **legítimo e de baixo risco intrínseco**. No entanto, ele possui um **risco operacional ALTO como vetor indireto de ameaças**. Sua confiabilidade e ubiquidade são exploradas por atores maliciosos para:

- **Ofuscar infraestrutura:** Apontar domínios maliciosos para ele, usando respostas 403 da Cloudflare como camada de defesa ou desvio.
- **Facilitar campanhas:** Servir como ponto de contato em cadeias de redirecionamento de phishing e fraudes.
- **Ocultar origens:** Ser utilizado como saída de VPN/Proxy, mascarando a origem real de ataques.

O IP em si não está comprometido, mas é um **instrumento passivo e amplamente utilizado no ecossistema de ameaças**.

---

3. Superfície de Ataque

3.1 Portas abertas / Serviços

Com base na análise do Netlas e na função conhecida do IP:

- **53/TCP/UDP**: DNS (Serviço de resolvedor público 1.1.1.1)
- **80/TCP**: HTTP (Redireciona para HTTPS)
- **443/TCP**: HTTPS (Serviço DNS sobre HTTPS/HTTP/3)

3.2 Vulnerabilidades (CVEs) detectadas

- **Nenhuma vulnerabilidade (CVE)** foi reportada nas fontes consultadas para os serviços deste IP.
- O risco não está em vulnerabilidades do próprio software da Cloudflare, mas no **padrão de abuso da infraestrutura**.

---

4. Informações de Rede e Geográficas

Campo	Valor
ASN	**AS13335 – Cloudflare, Inc.**
ISP / Provedor	**Cloudflare, Inc.** (Em parceria com a APNIC para o serviço 1.1.1.1)
Localização (Registro)	Austrália (AU) / Oceania. *(Devido ao Anycast, a localização de resposta varia; exemplo de roteamento para GRU-São Paulo observado)*
Tipo de Rede	Data-center / Anycast Network de Infraestrutura Global. Sinalizado como VPN/Proxy por algumas ferramentas.
Faixa de IP	Parte do bloco administrado pela Cloudflare e APNIC.
Domínios Principais	`one.one.one.one`, `cloudflare-dns.com`

5. Recomendações (próximos passos)

1. **Contextualizar Alertas:** Em logs de segurança (firewall, proxy, DNS), **não bloquear 1.1.1.1 por padrão**, pois é um serviço essencial. Em vez disso, investigar o **contexto** da conexão:
    - É uma consulta DNS legítima? (Comportamento esperado).
    - O tráfego HTTP/HTTPS para 1.1.1.1 está associado a tentativas de acesso a **domínios maliciosos** conhecidos? (Verificar logs de URL).
2. **Monitorar Domínios Associados:** Utilizar a lista de milhares de domínios associados a este IP (ex: via Netlas) como **IOCs (Indicadores de Comprometimento)**. Focar investigações nos domínios com padrões suspeitos.
3. **Correlacionar com Intenção Maliciosa:** Em casos de detecção de phishing ou fraude, verificar se a cadeia de redirecionamento inclui respostas 403/error pages da Cloudflare (IP 1.1.1.1). Isso é um **padrão tático** a ser documentado.
4. **Ajustar Regras de Detecção:** Criar regras em SIEM/IDS que destaquem conexões **HTTP/HTTPS não-DNS** para 1.1.1.1 a partir de estações de trabalho internas, pois isso é anômalo e pode indicar tráfego malicioso ofuscado.
5. **Acompanhar Reputação Dinâmica:** Manter o IP em monitoramento passivo em ferramentas como AbuseIPDB e VirusTotal para detectar qualquer mudança futura em seu status de reputação.

---

6. Considerações Finais

O IP **1.1.1.1** representa um caso clássico de **"infraestrutura dual-use"**: um ativo de rede crítico e legítimo que é simultaneamente **explorado massivamente por atores de ameaças para dar resiliência e ofuscar suas operações**. A avaliação de risco deve separar:

- **Risco Direto (BAIXO):** O IP não está comprometido, não hospeda malware e fornece um serviço público válido.
- **Risco Indireto / Associativo (ALTO):** O IP é um componente frequente em cadeias de ataque, servindo como cortina de fumaça ou ponto de rendez-vous para atividades maliciosas.

A recomendação principal é **entender e monitorar os padrões de abuso** deste IP, focando nos domínios e no contexto do tráfego associado a ele, em vez de tentar bloquear o próprio endereço.