Relatório de Threat Intelligence – Domínio **teste.com**

> **Fonte dos dados**: WHOIS, urlscan.io, VirusTotal API v3, AlienVault OTX, Análise DNS, cURL, crt.sh, Listas de Phishing.
> **Timestamp da Análise**: 2026-02-14T13:49:21.417489.

1. Resumo Executivo

O domínio `teste.com`, registrado em 2001, apresenta múltiplos indicadores fortes de atividade maliciosa. O uso de serviço de privacidade (Domains By Proxy, LLC) e, mais criticamente, nameservers personalizados associados a um domínio não corrente (`giantpanda.com`) apontam para uma infraestrutura projetada para operações maliciosas. A análise de comportamento revela seu uso ativo em campanhas de **malvertising, adware e phishing**, com uma extensa rede de subdomínios utilizados para typosquatting e redirecionamentos maliciosos. O domínio é detectado como **malicioso** pela Fortinet e **suspicious** por outras engines no VirusTotal. O padrão de emissão de certificados SSL para inúmeros subdomínios sequenciais reforça a tática de infraestrutura descartável para ataques. Embora não listado ativamente em feeds de phishing no momento da análise, a combinação dos IOCs (IPs, ASNs, padrão de certificados) e comportamentos observados classifica este domínio como um **risco alto** para organizações.

2. Análise de Comportamento

Fonte	Evidência	Interpretação
WHOIS	Registro privado (Domains By Proxy, LLC) e nameservers personalizados (`damao.ns.giantpanda.com`, `yangguang.ns.giantpanda.com`).	Prática comum para ocultação de identidade. Nameservers atípicos associados a um domínio não corrente são um forte IOC de infraestrutura maliciosa (C2, hospedagem fraudulenta).
urlscan.io	Histórico extenso de scans. Subdomínios de typosquatting (ex: `action.att.com.teste.com`, `www.climatempo.teste.com`). Redirecionamentos para landing pages (`www6.teste.com`) com parâmetros de tracking (PPC malicioso).	Padrão operacional claro de **malvertising** e **adware**. A rede de subdomínios é usada para imitar marcas legítimas e direcionar tráfego para páginas de anúncios fraudulentos ou distribuição de malware.
VirusTotal	**1 detecção como Malicious** (Fortinet) e **3 como Suspicious** (alphaMountain.ai, CyRadar, Forcepoint). IOCs: IPs `74.207.241.245`, `192.155.84.236` e os nameservers suspeitos.	Confirmação por múltiplas engines de segurança de comportamento anômalo ou associação a ameaças. A reputação é efetivamente negativa na comunidade de threat intelligence.

Fonte	Evidência	Interpretação
AlienVault OTX	Contagem zero de pulsos, listas vazias de malware e adversários associados.	Ausência de reputação negativa nesta plataforma específica. **Não exclui** a malícia evidenciada por outras fontes mais técnicas; pode indicar uma campanha mais recente ou não amplamente reportada em feeds comunitários.
Análise DNS	Resolve para IPs `96.126.111.165` e `66.175.209.179` com TTL baixo (~376s).	TTL baixo pode facilitar técnicas de **fast-flux**, comuns em redes de botnets e phishing para rápida troca de IPs e evasão de bloqueios.
Análise HTTP (cURL)	Servidor responde apenas via **HTTP** (inseguro), sem redirecionamento para HTTPS. Código 200.	Ausência de criptografia facilita ataques **man-in-the-middle** e é um indicador de infraestrutura de baixa qualidade, frequentemente associada a páginas de phishing ou distribuição de malware.
Análise de Certificado (crt.sh)	Histórico extenso de certificados (Let's Encrypt, ZeroSSL) para subdomínios sequenciais (www1, www6, www42, www70) e wildcard (*.teste.com).	Padrão clássico de infraestrutura de **phishing**, onde certificados são emitidos massivamente para subdomínios descartáveis que hospedam páginas fraudulentas. Indica operação ativa e intencional.
Listas de Phishing	Não detectado em listas ativas consultadas.	A ausência não é um indicador de benignidade. Campanhas de phishing são efêmeras e o domínio pode estar entre ciclos de listagem ou usando subdomínios não rastreados.

Existem fortes evidências de que este domínio está ou esteve envolvido em operações maliciosas:

- **Associação a Campanhas de Malvertising/Adware:** Uso de uma rede de subdomínios para typosquatting e redirecionamento de tráfego para landing pages com anúncios maliciosos ou fraudes de clique (PPC malicioso).
- **Infraestrutura para Phishing:** Padrão de emissão de certificados SSL para subdomínios numerados e genéricos, combinado com nameservers anômalos, é altamente sugestivo de preparação para ou execução de campanhas de phishing.
- **Potencial C2 ou Hospedagem Maliciosa:** Configuração de DNS atípica (nameservers personalizados em domínio morto) e detecções por engines de antivírus como Fortinet sugerem possível uso para comando e controle (C2) ou hospedagem de payloads.

Táticas/Procedimentos (ATT&CK) observados:

- **T1583.001 – Acquire Infrastructure: Domains** (Registro com privacidade e nameservers personalizados).
- **T1608.001 – Stage Capabilities: Upload Malware** (Possível hospedagem em subdomínios).

- **T1189 – Drive-by Compromise** (Redirecionamentos via malvertising).
- **T1566 – Phishing** (Uso de subdomínios para imitar marcas legítimas).
- **T1573 – Encrypted Channel** (Uso de certificados SSL – mesmo que de autoridades gratuitas – para criptografar tráfego malicioso).
- **T1595 – Active Scanning** (Possível uso de subdomínios para sondagem).

3. Informações de Rede e Geográficas

Campo	Valor
IPs Resolvidos (A)	`96.126.111.165`, `66.175.209.179`, `74.207.241.245`, `192.155.84.236`
ASN / Provedor (ISP)	`AS63949` (Akamai-Linode), `AS16509` (Amazon.com, Inc.), `AS20473` (AS-CHOOPA). Hospedagem em infraestrutura de cloud/comercial.
Localização (Baseado nos IPs)	Primariamente **Estados Unidos** (dados de geolocalização para os IPs de hospedagem).
Nameservers	`damao.ns.giantpanda.com`, `yangguang.ns.giantpanda.com` (Domínio pai `giantpanda.com` não corrento – **IOC Forte**).
Protocolo Web	Apenas HTTP (inseguro). Sem HTTPS forçado.
DNSSEC	Não assinado (ausente).

4. Domínios e IPs Relacionados

- **Subdomínios Maliciosos (Exemplos):** `action.att.com.teste.com`, `www.climatempo.teste.com`, `www1.teste.com`, `www6.teste.com`, `www42.teste.com`, `www70.teste.com`. (Padrão indica centenas possíveis).
- **IPs de Infraestrutura:** `96.126.111.165`, `66.175.209.179`, `74.207.241.245`, `192.155.84.236`.
- **Nameserver Pai Suspeito:** `giantpanda.com` (Domínio não funcional associado à infraestrutura de DNS maliciosa).

5. Recomendações de Ações de Investigação

1. **Bloqueio Imediato:** Recomenda-se o bloqueio proativo do domínio `teste.com` e todos os seus subdomínios (padrão `*.teste.com`) em firewalls, proxies web e soluções de DNS seguro (sinkhole).
2. **Hunting em Logs:** Buscar em logs de DNS, proxy e firewall por qualquer conexão para os IPs listados (`96.126.111.165`, `66.175.209.179`, etc.) e resoluções para qualquer subdomínio de `teste.com`.
3. **Monitoramento de Certificados:** Incluir o padrão `*.teste.com` em monitoramentos que alertem para a emissão de novos certificados SSL para estes domínios, indicando potencial expansão da infraestrutura de ataque.
4. **Análise de Endpoints:** Realizar buscas por hashes de arquivos (ex: scripts JS, executáveis) que possam ter sido baixados de qualquer um dos subdomínios ou IPs associados.
5. **Inteligência Contextual:** Investigar o ASN `AS63949` (Akamai-Linode) e o domínio `giantpanda.com` em outras fontes de threat intelligence para identificar campanhas ou atores relacionados que utilizem a mesma infraestrutura base.
6. **Conscientização:** Alertar usuários sobre o risco de domínios com nomes genéricos como "teste" e a prática de typosquatting, já que este domínio imita serviços legítimos em sua estrutura de

subdomínios.

6. Conclusão

O domínio `teste.com` não é um domínio benigno ou de teste legítimo. Ele opera como uma **infraestrutura maliciosa ativa**, envolvida principalmente em esquemas de **malvertising/adware** e com fortes indícios de preparação para **campanhas de phishing** em escala. A combinação de registros de privacidade, nameservers anômalos, padrão de certificados revelador e detecções positivas em ferramentas de segurança consolida sua classificação como uma **ameaça de alto risco**. Ações de bloqueio preventivo e investigação profunda no ambiente são altamente recomendadas para mitigar riscos de comprometimento e perda de dados.