Relatório Técnico OSINT - Exposição de Superfície de Ataque

Status: Coleta concluída

Severidade: Alta

Tipo: Information Exposure / Attack Surface Enumeration / OSINT Recon

Contexto

Uma análise OSINT passiva foi conduzida sobre uma organização privada (identidade redigida) com foco em:

- Mapeamento de superfície de ataque

- Identificação de dados expostos

- Coleta de metadados públicos

- Possíveis vetores de engenharia social

- Riscos associados a má configuração e excesso de exposição digital

Nenhum acesso não autorizado foi realizado.

WHOIS Informações Públicas (Suprimido)

Dados institucionais

Razão Social: [Suprimido]

Responsável Técnico: [Suprimido]

CNPJ: Suprimido

Localização: Suprimido

Contato administrativo encontrado

NIC-HDL: Suprimido

Pessoa: Suprimido

E-mail: Suprimido

Registro RDAP

Fonte analisada: https://rdap.registro.br/domain/[Suprimido]

Descrição: logs públicos de registro, DNS, servidores, registros de alteração.

Cookies Identificados (Suprimido)

Todos não-secure, alguns persistentes:

- ar_debug = 1
- _gcl_gs = [...]
- _gcl_aw = [...]
- _gcl_au = [...]
- _ga_0H87VQ8PLE = [...]
- _ga = [...]
- _dsk = [...]
- _clck = [...]

Observação: ausência de Secure + HttpOnly aumenta risco de roubo caso esteja em ambiente inseguro ou XSS no domínio.

Subdomínios Encontrados (Suprimido)

Subdomínios operacionais

- cpanel.[Suprimido]
- api.[Suprimido]
- developer.caf.[Suprimido]
- sgc.caf.[Suprimido]
- shteste.[Suprimido]
- brain.[Suprimido]
- intranet.[Suprimido]

Subdomínio recente

- brain.[REDACTED] - nginx/1.18.0 (Ubuntu)

Tecnologias Identificadas (Fingerprinting)

Frameworks, CDNs e SDKs externos:

Next.js, Cloudflare, CloudFront CDN, Datadog RUM, Facebook Pixel, Google Analytics, TikTok Pixel, Reddit Conversion Tracking, Segment, Apollo GraphQL, Styled Components, Java EE, OpenResty, Apache, Nginx Ubuntu 1.18.0

Riscos gerais:

Ampla superfície de third-parties, supply chain, fingerprinting detalhado, correlação entre ambientes.

Vulnerabilidades - NGINX

Versão: NGINX 1.18.0 (Ubuntu)

CVEs:

CVE-2021-23017, CVE-2021-3618, CVE-2020-11724

Exploits possíveis:

HTTP/2 Request Flooding, Resolver DoS, RCE hipotético.

Painéis e Sistemas Expostos

Painel CPanel: https://cpanel.[SUPRIMIDO]

Arquivo info.php exposto: https://shteste.[SUPRIMIDO]/info.php

API pública: https://api.[SUPRIMIDO]

Sistema de Gestão CAF: https://sgc.caf.[SUPRIMIDO]

Portal de desenvolvedores: https://developer.caf.[SUPRIMIDO]

Endereços IP Encontrados (SUPRIMIDO)

- 34.[SUPRIMIDO].[SUPRIMIDO].[SUPRIMIDO]

- 177.[SUPRIMIDO].[SUPRIMIDO].[SUPRIMIDO]

Arquivos PDF internos encontrados (SUPRIMIDO)

Treinamentos internos, rotinas administrativas, regulamentos, processos internos.

Perfis suspeitos encontrados (SUPRIMIDO)

Perfis inconsistentes e redigidos.

Exposição de Contatos de Funcionários

E-mails e telefones públicos encontrados.

Reclamações Públicas

Cobrança indevida, diploma atrasado, problemas de matrícula, curso abaixo do esperado.

Conclusão Geral

A organização apresenta:

- subdomínios expostos
- sistemas sem autenticação
- arquivos sensíveis públicos
- painéis administrativos visíveis
- dados internos em PDFs públicos
- dados pessoais expostos
- CVEs conhecidos afetando versões
- cookies inseguros
- exposição excessiva de tecnologias
- info.php revelando estrutura interna

Severidade final: Alta.