Faculdade Adventista
BAHIA

RELATÓRIO DE PENTESTING

Orientador: Jean do Ouro

Revisado pela última vez em: 30/11/2022

ÍNDICE

1. SUMÁRIO EXECUTIVO

Este relatório reflete os resultados da análise de vulnerabilidades da plataforma (aplicações web) BackBlaze (https://backblaze.com/). A análise de vulnerabilidade foi realizada no período de 26 de novembro a 30 de novembro de 2022.

1.1 Sobre Projeto de Desenvolvimento Profissional

Projeto desenvolvido por alunos da Faculdade Adventista da Bahia para encontrar vulnerabilidades em aplicações web de empresas participantes do programa Bugcrowd, a plataforma de segurança coletiva mais inteligente do setor, que utiliza Crowdsourced Security para eliminar desequilíbrios utilizando pesquisadores de segurança da Whitehat para encontrar e remover vulnerabilidades.

1.2 Código de Ética

Os alunos que concluintes do curso de Gestão de Tecnologia da Informação da Faculdade Adventista da Bahia aplicam e aderem aos seguintes princípios:

• Integridade: a honestidade dos pentesters constrói confiança e, portanto, forma a base da confiança em seus julgamentos;

• Objetividade: os pentesters experientes têm a maior objetividade profissional ao coletar, avaliar e comunicar informações relacionadas à atividade ou processo sob investigação, têm uma avaliação equilibrada de todas as circunstâncias importantes do ponto de vista de sua própria análise e não são indevidamente influenciados por seus próprios interesses ou por outros na formação de julgamentos;

• Confidencialidade: os pentesters respeitam o valor e a propriedade das informações que recebem e não divulgam informações sem a devida autoridade, a menos que haja uma obrigação legal ou profissional de fazê-lo;

• Competência: os pentesters aplicam os conhecimentos, habilidades e experiência necessários no desempenho dos serviços de análise de vulnerabilidades e testes de intrusão.

2. INTRODUÇÃO

Foi realizado análises de vulnerabilidades na plataforma BackBlaze, conforme definido no "Escopo" deste relatório, cujos resultados serão abordados adiante. Os testes de segurança foram realizados no período de 26/11/2022 a 30/11/2022 e seu objetivo foi identificar vulnerabilidades e propor recomendações para sua correção. As fragilidades identificadas foram avaliadas e priorizadas de acordo com seu risco relativo e medidas para sua remediação também foram propostas.

2.1 Termo de responsabilidade

Todo o trabalho de avaliação para a elaboração deste documento foi realizado de acordo com as práticas de mercado e em conformidade com as obrigações e regulamentos impostos tanto pela legislação vigente, quanto pelo que foi estabelecido pelo orientador Jean Ouro.
As informações contidas neste relatório estão sujeitas e limitadas pelas condições descritas nas seções de “Escopo” e “Objetivos” e conforme as condições acordadas para a realização das atividades de análise de vulnerabilidades.
Em qualquer auditoria ou avaliação autorizada, o tempo e os recursos são naturalmente limitados e, portanto, quando comparado ao tempo e recursos potencialmente ilimitados disponíveis para partes com intenção maliciosa, a existência de vulnerabilidades será verificada, mas a inexistência de todos e quaisquer tipos de fragilidades não pode ser assegurado absolutamente.
Neste contexto, embora tenham sido feitos todos os esforços para auditar e avaliar a segurança do ambiente computacional da Tamedia, este relatório não garante de forma alguma o estabelecimento de um sistema impenetrável. Sendo assim, a FADBA e os pentesters não se responsabilizam por qualquer perda ou dano direto ou indireto causado por qualquer falha ou violação dos sistemas desta da plataforma de viagem.
Por fim, as informações deste relatório têm classificação PÚBLICA e devem ser usadas apenas pela BackBlaze e pela FADBA, sendo de inteira e única responsabilidade de ambas.

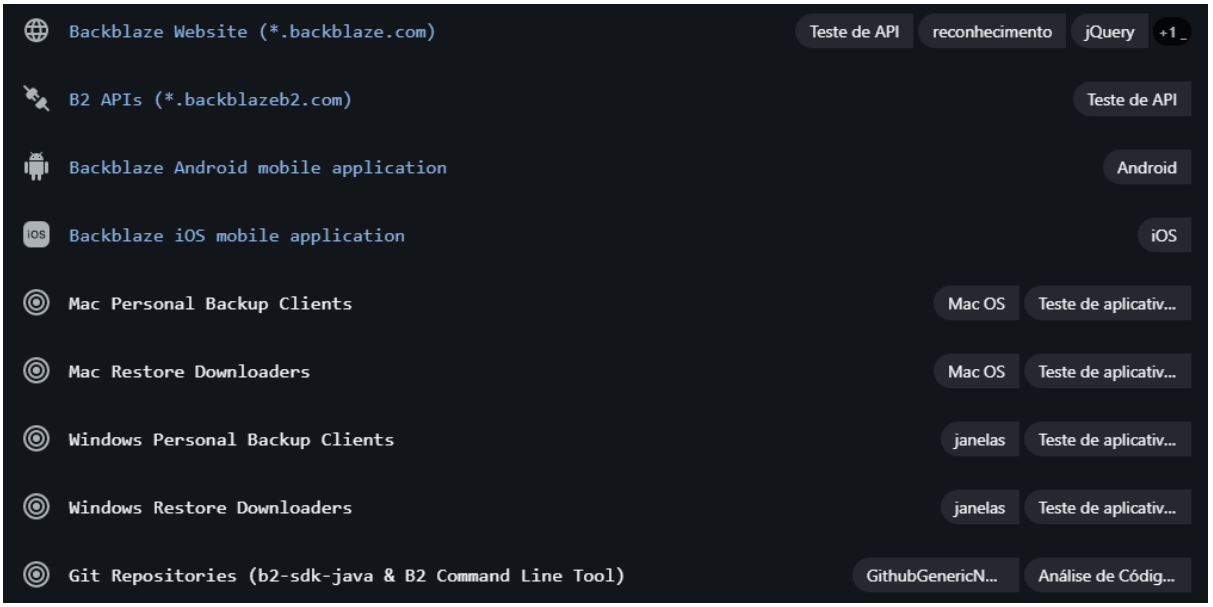
2.2 Análise da organização

Backblaze, Inc. é uma empresa americana de armazenamento em nuvem e backup de dados com sede em San Mateo, Califórnia. Fundada em 2007 por Gleb Budman, Billy Ng, Nilay Patel, Brian Wilson, Tim Nufire, Damon Uyeda e Casey Jones, seus dois principais produtos são os serviços de Armazenamento em Nuvem B2 e Backup Computacional, direcionados aos mercados comercial e pessoal.

2.3 Objetivo

O objetivo dos testes foi fornecer informações confiáveis sobre a segurança do ambiente computacional da Tamedia. Dessa forma, a avaliação identificou vulnerabilidades e quantificou sua criticidade, para que as mesmas possam ser geridas, resolvidas e, consequentemente, ajudar a prevenir o mau funcionamento e/ou perda financeira por meio de fraudes, fornecer diligências a regulações a clientes, e proteger a marca contra a perda de reputação.

2.4 Escopo



Os testes realizados foram do tipo “Gray Box” e seguiram uma abordagem com base nos limites impostos pela empresa. Portanto, o principal objetivo alcançado através da adoção de metodologia, detalha adiante, que consistiu em priorizar e otimizar as validações realizadas, fornecendo garantias em termos de cobertura ao minimizar as chances de uma falha evidente escapar ao processo de análise. Ademais, foram reunidas informações sobre a organização para que seja possível determinar o ambiente em que ela opera e a relevância desse ambiente para o processo de gestão de riscos de segurança da informação. Nesse sentido, foram realizados testes básicos de verificação de segurança em IPs obtidos indiretamente, isto é, IPs que são públicos e que foram conseguidos através de consulta ao “DNSdumpster” e “Spiderfoot”, ferramentas de pesquisa de domínio gratuitas que visam descobrir hosts relacionados a um domínio, conforme mostrados na Figura 1 e 2.

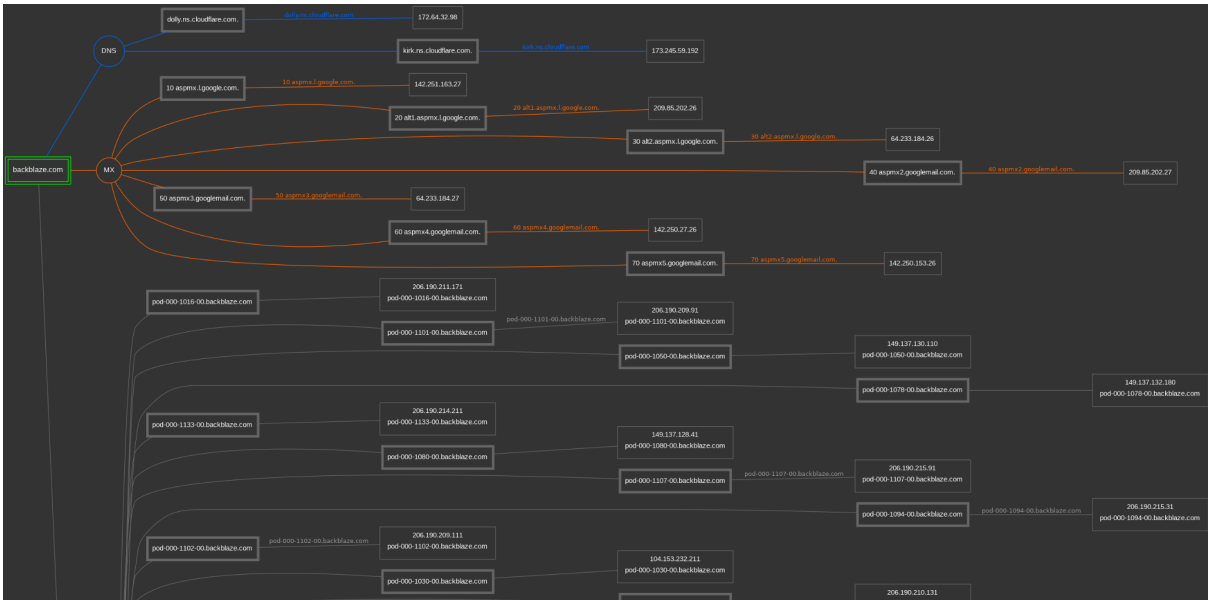


Figura 1 - Mapeamento dos endereços IP para o domínio “backblaze.com”

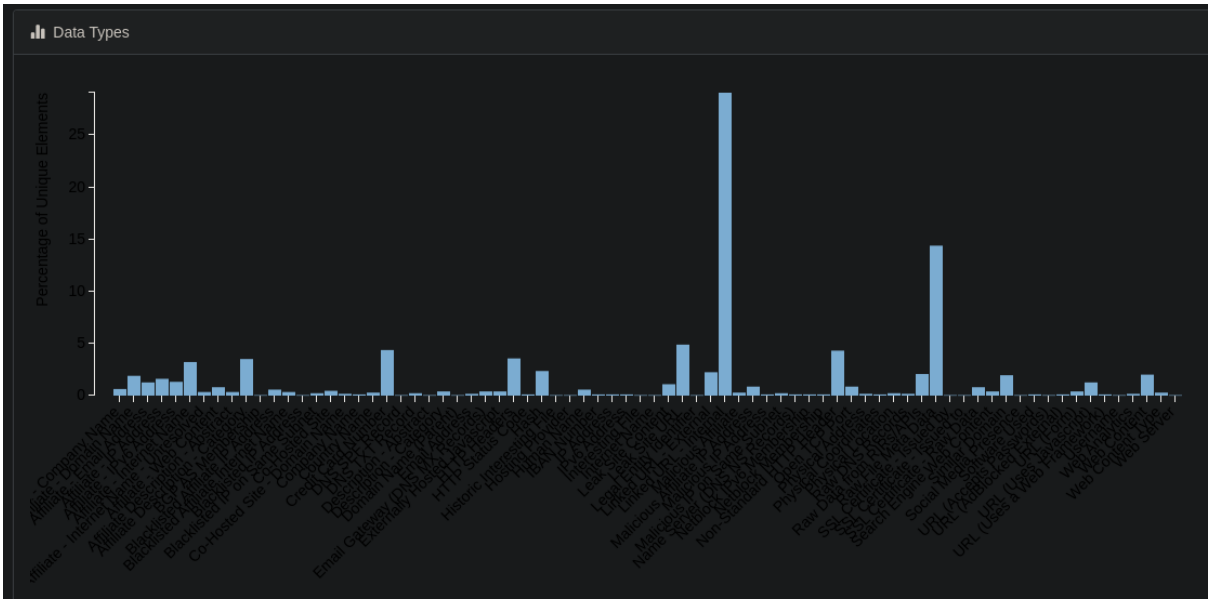


Figura 2 Mapeamento de IP feito pelo Spiderfoot

2.5 Limites

Todos os devidos cuidados foram tomados com base na especificação e critérios da empresa (Backblaze) e as orientações do professor (Jean Ouro - FADBA) para não prejudicar o funcionamento da empresa, a fim de não causar impacto em seus sistemas ou interferir nos negócios diários da plataforma.

Não fazem parte do escopo:

- ➔ Ataques de negação de serviço (DoS) que apenas sobrecarregam os recursos (em oposição a travar sistemas)
- ➔ Preocupações com as melhores práticas não acompanhadas por explorações no escopo (por exemplo, cabeçalhos HTTP ausentes, software desatualizado, etc.)
- ➔ Problemas genéricos de falsificação de e-mail
- ➔ Vulnerabilidades em terceiros usando Backblaze
- ➔ Qualquer vulnerabilidade obtida de uma conta comprometida
- ➔ Vulnerabilidades resultantes de computadores clientes ou navegadores inseguros ou comprometidos (por exemplo, um laptop roubado sem senha, malware preexistente, etc.)
- ➔ Vulnerabilidades que dependem de usuários que exibem práticas de segurança abaixo do padrão (por exemplo, exibição de credenciais em locais públicos, falha ao sair de um computador compartilhado, etc.)

➔ Ataques físicos contra nossa infraestrutura, instalações e escritórios

➔ Ataques de engenharia social, incluindo aqueles direcionados a funcionários, contratados e fornecedores

3. DETALHAMENTO DOS DADOS DO SITE E SUBDOMÍNIOS

1 - Whois

Whois Record for BackBlaze.com

− Domain Profile

Registrant	REDACTED FOR PRIVACY (DT)
Registrant Org	DATA REDACTED
Registrant Country	us
Registrar	Cloudflare, Inc. CloudFlare, Inc. IANA ID: 1910 URL: https://www.cloudflare.com,http://www.cloudflare.com Whois Server: whois.cloudflare.com registrar-abuse@cloudflare.com (p) 14153197517
Registrar Status	clientTransferProhibited, clienttransferprohibited
Dates	5,722 days old Created on 2007-04-02 Expires on 2026-04-02 Updated on 2021-11-22
Name Servers	DOLLY.NS.CLOUDFLARE.COM (has 26,848,757 domains) KIRK.NS.CLOUDFLARE.COM (has 26,848,757 domains)
Tech Contact	REDACTED FOR PRIVACY (DT) DATA REDACTED DATA REDACTED, DATA REDACTED, DATA REDACTED, DATA REDACTED, DATA REDACTED (p) x (f) x
IP Address	104.17.5.3 - -1 other site is hosted on this server
IP Location	- California - San Jose - Cloudflare Inc.
ASN	AS13335 CLOUDFLARENET, US (registered Jul 14, 2010)
Domain Status	Registered And Active Website
IP History	23 changes on 23 unique IP addresses over 15 years
Registrar History	2 registrars with 2 drops
Hosting History	9 changes on 8 unique name servers over 15 years

− Website

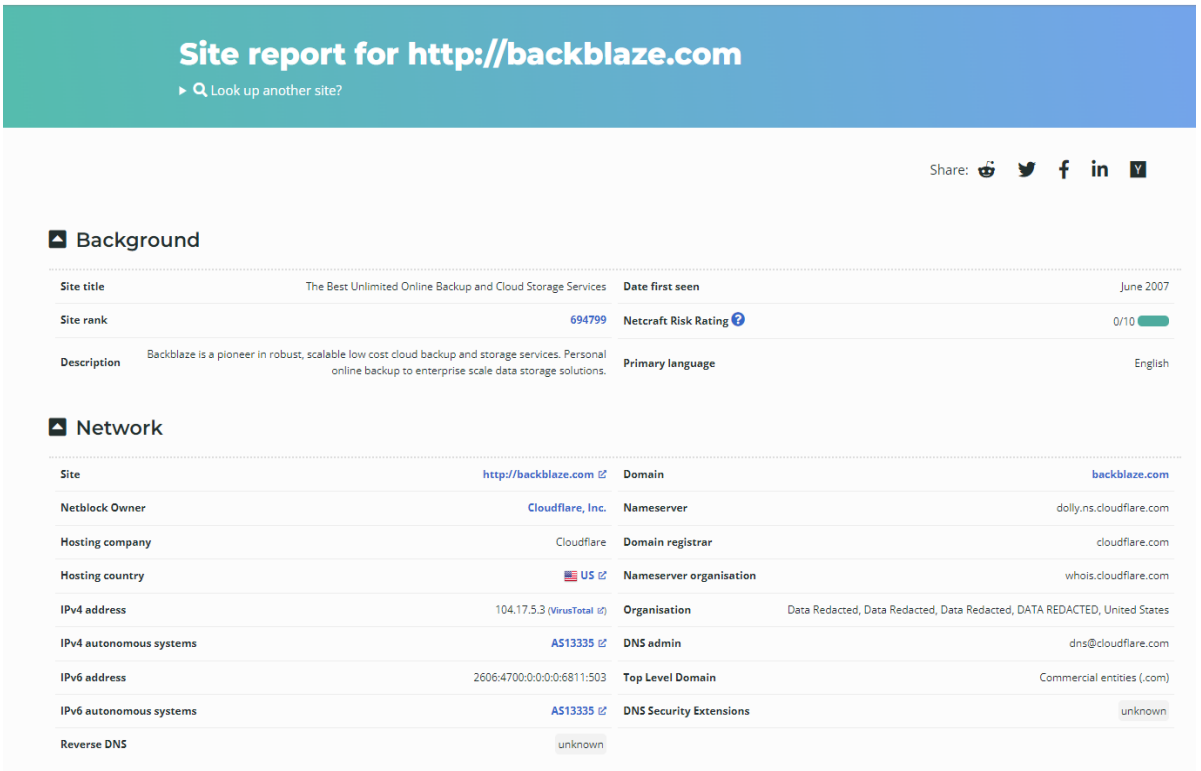
Website Title	500 SSL negotiation failed:
Response Code	500

Whois Record (last updated on 2022-12-01)

```
Domain Name: backblaze.com
Registry Domain ID: 906551926_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.cloudflare.com
Registrar URL: https://www.cloudflare.com
        http://www.cloudflare.com
Updated Date: 2021-11-22T09:44:23+00:00
        2021-11-22
Creation Date: 2007-04-02T23:23:41+00:00
        2007-04-02
Registrar Registration Expiration Date: 2026-04-02T23:23:41+00:00
        2026-04-02
Registrar: Cloudflare, Inc.
        CloudFlare, Inc.
Sponsoring Registrar IANA ID: 1910
Registrar Abuse Contact Email:  registrar-abuse@cloudflare.com
Registrar Abuse Contact Phone: 14153197517
Status:
        clientTransferProhibited
        clienttransferprohibited
Registry Registrant ID:
Registrant Name: REDACTED FOR PRIVACY (DT)
Registrant Organization: DATA REDACTED
Registrant Street: DATA REDACTED
Registrant City: DATA REDACTED
Registrant State/Province: CA
Registrant Postal Code: DATA REDACTED
Registrant Country: us
Registrant Phone:
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: REDACTED FOR PRIVACY (DT)
Registry Admin ID:
Admin Name: REDACTED FOR PRIVACY (DT)
Admin Organization: DATA REDACTED
Admin Street: DATA REDACTED
Admin City: DATA REDACTED
Admin State/Province: DATA REDACTED
Admin Postal Code: DATA REDACTED
Admin Country: DATA REDACTED
Admin Phone:
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: REDACTED FOR PRIVACY (DT)
```

```
Registry Tech ID:
Tech Name: REDACTED FOR PRIVACY (DT)
Tech Organization: DATA REDACTED
Tech Street: DATA REDACTED
Tech City: DATA REDACTED
Tech State/Province: DATA REDACTED
Tech Postal Code: DATA REDACTED
Tech Country: DATA REDACTED
Tech Phone:
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: REDACTED FOR PRIVACY (DT)
Registry Billing ID:
Billing Name: REDACTED FOR PRIVACY (DT)
Billing Organization: DATA REDACTED
Billing Street: DATA REDACTED
Billing City: DATA REDACTED
Billing State/Province: DATA REDACTED
Billing Postal Code: DATA REDACTED
Billing Country: DATA REDACTED
Billing Phone:
Billing Phone Ext:
Billing Fax:
Billing Fax Ext:
Billing Email: REDACTED FOR PRIVACY (DT)
Nameservers:
        dolly.ns.cloudflare.com
        kirk.ns.cloudflare.com
DNSSEC: unsigned
```

2 - Netcraft



Site report for http://backblaze.com

▸ Look up another site?

Share:

Background

Site title	The Best Unlimited Online Backup and Cloud Storage Services	**Date first seen**	June 2007
Site rank	694799	**Netcraft Risk Rating**	0/10
Description	Backblaze is a pioneer in robust, scalable low cost cloud backup and storage services. Personal online backup to enterprise scale data storage solutions.	**Primary language**	English

Network

Site	http://backblaze.com	**Domain**	backblaze.com
Netblock Owner	Cloudflare, Inc.	**Nameserver**	dolly.ns.cloudflare.com
Hosting company	Cloudflare	**Domain registrar**	cloudflare.com
Hosting country	US	**Nameserver organisation**	whois.cloudflare.com
IPv4 address	104.17.5.3 (VirusTotal)	**Organisation**	Data Redacted, Data Redacted, Data Redacted, DATA REDACTED, United States
IPv4 autonomous systems	AS13335	**DNS admin**	dns@cloudflare.com
IPv6 address	2606:4700:0:0:0:0:6811:503	**Top Level Domain**	Commercial entities (.com)
IPv6 autonomous systems	AS13335	**DNS Security Extensions**	unknown
Reverse DNS	unknown		

IP delegation

IPv4 address (104.17.5.3)

IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
↳ 104.0.0.0-104.255.255.255	United States	NET104	American Registry for Internet Numbers
↳ 104.16.0.0-104.31.255.255	United States	CLOUDFLARENET	Cloudflare, Inc.
↳ 104.17.5.3	United States	CLOUDFLARENET	Cloudflare, Inc.

IPv6 address (2606:4700:0:0:0:0:6811:503)

IP range	Country	Name	Description
::/0	N/A	ROOT	Root inet6num object
↳ 2600::/12	United States	NET6-2600	American Registry for Internet Numbers
↳ 2606:4700::/32	United States	CLOUDFLARENET	Cloudflare, Inc.
↳ 2606:4700:0:0:0:0:6811:503	United States	CLOUDFLARENET	Cloudflare, Inc.

SSL/TLS

This is not a HTTPS site. If you're looking for SSL/TLS information try the **HTTPS site report**.

Hosting History

Netblock owner	IP address	OS	Web server	Last seen
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.17.5.3	unknown	cloudflare	18-Aug-2022
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.17.5.3	Linux	cloudflare	15-Aug-2022
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.17.6.3	unknown	cloudflare	13-Aug-2022
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.17.6.3	Linux	cloudflare	12-Aug-2022
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.17.5.3	Linux	cloudflare	11-Aug-2022
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.17.6.3	unknown	cloudflare	9-May-2022
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.17.5.3	unknown	cloudflare	6-May-2022
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.17.6.3	unknown	cloudflare	5-May-2022
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.17.5.3	unknown	cloudflare	4-May-2022
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.17.6.3	Linux	cloudflare	10-Apr-2022

Sender Policy Framework

A host's Sender Policy Framework (SPF) describes who can send mail on its behalf. This is done by publishing an SPF record containing a series of **rules**. Each rule consists of a qualifier followed by a specification of which domains to apply this qualifier to. For more information please see **open-spf.org**.

Qualifier	Mechanism	Argument
+ (Pass)	ip4	50.31.32.0/19
+ (Pass)	ip4	50.196.177.12/30
+ (Pass)	ip4	54.174.63.52/31
+ (Pass)	ip4	64.18.0.0/20
+ (Pass)	ip4	64.233.160.0/19
+ (Pass)	ip4	66.102.0.0/20
+ (Pass)	ip4	66.249.80.0/20
+ (Pass)	ip4	72.14.192.0/18
+ (Pass)	ip4	74.125.0.0/16
+ (Pass)	ip4	85.222.130.192/26
+ (Pass)	ip4	85.222.138.192/26
+ (Pass)	include	spf1.backblaze.com
~ (SoftFail)	all	

DMARC

DMARC (Domain-based Message Authentication, Reporting and Conformance) is a mechanism for domain owners to indicate how mail purporting to originate from their domain should be authenticated. It builds on SPF and DKIM, providing a method to set policy and to give reporting of failures. For more information please see **dmarc.org**.

Raw DMARC record:

```
v=DMARC1; p=none; pct=100; rua=mailto:re+beyibhsql3t@dmarc.postmarkapp.com; sp=none; aspf=r;
```

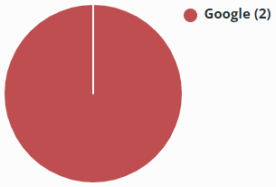
Tag	Field	Value
p=none	Requested handling policy	None: no specific action to be taken regarding delivery of messages.
pct=100	Sampling rate	100% of messages from the Domain Owner's mail stream should have DMARC applied.
rua=mailto:re+beyibhsql3t@dmarc.postmarkapp.com	Reporting URI(s) for aggregate data	re+beyibhsql3t@dmarc.postmarkapp.com
sp=none	Requested handling policy for subdomains	None: no specific action to be taken regarding delivery of messages.
aspf=r	SPF alignment mode	Relaxed: the Organizational Domains of both the SPF-authenticated domain and that of the RFC5322.From domain must be equal if the identifiers are to be considered aligned.

Web Trackers

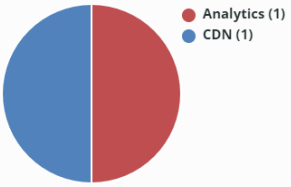
Web Trackers are third-party resources loaded onto a webpage. Trackable resources include social sharing widgets, javascript files, and images. These trackers can be used to monitor individual user behaviour across the web. Data derived from these trackers are primarily used for advertising or analytics purposes.

2 known trackers were identified.

Companies



Categories



Company	Primary Category	Tracker	Popular Sites with this Tracker
Google	**Analytics**	Googletagmanager	**www.foxnews.com**, **www.corriere.it**, **www.coingecko.com**
	CDN	Googlecdn	**www.infobae.com**, **www.nexusmods.com**, **www.taosamuebles.com**

Site Technology (fetched today)

HTTP Accelerator

A web accelerator is a proxy server that reduces web site access times.

Technology	Description	Popular sites using this technology
Cloudflare	Content delivery network and distributed domain name server service	**www.ecosia.org**, **www.canva.com**, **9gag.com**

Server-Side

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

Technology	Description	Popular sites using this technology
SSL	A cryptographic protocol providing communication security over the Internet	

Client-Side

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

Technology	Description	Popular sites using this technology
JavaScript	Widely-supported programming language commonly used to power client-side dynamic content on websites	

Client-Side Scripting Frameworks

Frameworks or libraries allow for easier development of applications by providing an Application Program Interface (API) or a methodology to follow whilst developing.

Technology	Description	Popular sites using this technology
Google Tag Manager	*No description*	**www.chess.com**, **www.inspq.qc.ca**, **www.nexusmods.com**
jQuery	A JavaScript library used to simplify the client-side scripting of HTML	**www.amazon.de**, **www.amazon.it**, **www.amazon.in**

Content Delivery Network

A content delivery network or content distribution network (CDN) is a large distributed system of servers deployed in multiple data centers in the Internet. The goal of a CDN is to serve content to end-users with high availability and high performance.

Technology	Description	Popular sites using this technology
Cloudflare	Content delivery network and distributed domain name server service	www.coingecko.com, www.notion.so, www.foxnews.com

Web Stats

Web analytics is the measurement, collection, analysis and reporting of internet data for purposes of understanding and optimizing web usage.

Technology	Description	Popular sites using this technology
Google Webmaster Tools	Set of tools allowing webmasters to check indexing status and optimize visibility of their websites on Google	www.qwant.com, www.ebay.com, www.roblox.com

Character Encoding

A character encoding system consists of a code that pairs each character from a given repertoire with something else such as a bit pattern, sequence of natural numbers, octets, or electrical pulses in order to facilitate the transmission of data (generally numbers or text) through telecommunication networks or for data storage.

Technology	Description	Popular sites using this technology
UTF8	UCS Transformation Format 8 bit	

HTTP Compression

HTTP compression is a capability that can be built into web servers and web clients to make better use of available bandwidth, and provide greater transmission speeds between both.

Technology	Description	Popular sites using this technology
Gzip Content Encoding	Gzip HTTP Compression protocol	www.newsit.gr, www.pravda.com.ua, www2.secure.hsbcnet.com

Web Browser Targeting

Web browser targeting enables software applications to make use of specific functions of the browser as well as optimizing the application for specific browser versions.

Technology	Description	Popular sites using this technology
X-Content-Type-Options	Browser MIME type sniffing is disabled	www.msn.com, web.whatsapp.com, mail.google.com
Strict Transport Security	Web security policy mechanism whereby a web server declares that complying user agents are to interact with it using only secure HTTP connections	mail-redir.mention.com, stackoverflow.com, my308053-sso.crm.ondemand.com
X-Frame-Options Same Origin	Do not allow this site to be rendered within an iframe	www.baidu.com, www.google.com, teams.microsoft.com

Doctype

A Document Type Declaration, or DOCTYPE, is an instruction that associates a particular SGML or XML document (for example, a webpage) with a Document Type Definition (DTD).

Technology	Description	Popular sites using this technology
HTML5	Latest revision of the HTML standard, the main markup language on the web	
HTML	The main markup language used for displaying web pages within browsers	www.aliexpress.com, www.taosamuebles.com, www.startpage.com

HTML 5

HTML5 is a markup language for structuring and presenting content for the World Wide Web and a core technology of the Internet. It is the fifth revision of the HTML standard.

Technology	Description	Popular sites using this technology
Viewport meta tag	HTML5 tag usually used for mobile optimization	login.live.com, docs.microsoft.com

CSS Usage

Cascading Style Sheets (CSS) is a style sheet language used for describing the presentation semantics (the look and formatting) of a document written in a markup language (such as XHTML).

Technology	Description	Popular sites using this technology
CSS Media Query	*No description*	www.twitch.tv, www.w3schools.com, www.microsoft.com
Embedded	Styles defined within a webpage	www.amazon.com, www.amazon.ca, www.amazon.fr
External	Styles defined within an external CSS file	www.instagram.com, www.linkedin.com, www.netflix.com

3 - Robtex

ANÁLISE

Esta seção mostra uma análise rápida do nome do host ou número IP fornecido.

Backblaze .com tem dois servidores de nome, sete servidores de correio e dois números de IP.

Servidores de nome Cloudflare

Os servidores de nome são dolly.ns. **cloudflare** .com e kirk.ns. **cloudflare** . com .

Qual é a história por trás dos nomes dos servidores de nomes da CloudFlare? .

Googlemail e servidores de correio do Google

Os servidores de correio são aspmx2. **googlemail** . com , aspmx3 . **googlemail** . com , aspmx4 . **googlemail** . com , aspmx5 . **googlemail** . com , aspmx.l . google.com , **alt1.aspmx.l** . google.com e **alt2.aspmx.l** . **google** . com .

Este domínio usa o Google para lidar com seu e-mail.

números IP

Os números IP são 104.153.232.253 e 162.244.57.11 . O PTR dos números IP é 162.244.57.11.rdns. **backblaze** . com . Os números de IP estão nos Estados Unidos.

Resultados encontrados

Backblaze .ca , **backblaze** .cn , **backblaze** .co , **backblaze** .de , **backblaze** .es , **backblaze** .fr , **backblaze** .in , **backblaze** .info , **backblaze** .it , **backblaze** .jp , **backblaze** .me e **backblaze** .net .

INFORMAÇÃO RÁPIDA

Resumo rápido do nome do host

backblaze.com informações rápidas

Em geral	
FQDN	backblaze.com
Nome de anfitrião	
Nome do domínio	backblaze.com
Registro	com
TLD	com
DNS	
números IP	104.153.232.253 162.244.57.11
Servidores de nomes	dolly.ns. **cloudflare.com** kirk.ns. **cloudflare.com**
servidores de correio	aspmx2. **googlemail.com** aspmx3. **googlemail.com** aspmx4. **googlemail.com** aspmx5. **googlemail.com** aspmx.l. **google.com** alt1.aspmx.l. **google.com** alt2.aspmx.l. **google.com**

REGISTROS

Análise hierárquica da entidade

backblaze .com

- uma 104.153.232.253
  - quem é Backblaze Inc (BACKB-7)
  - rota 104.153.232.0/23
  - bgp AS32354
  - descrição FAPVPS-NET-2
  - localização Brooklin, Estados Unidos
- 162.244.57.11
  - quem é Sem fio (UNWIR-1)
  - descrição Unwired Ltd +1-510-868-1614
  - localização Berkeley, Estados Unidos
  - ptr 162.244.57.11.rdns. **backblaze** .com
- ns dolly.ns. **cloudflare.com**
  - uma 2400:cb00:2049:1::adf5:3a62
    - rota 2400:cb00:2049::/48
    - bgp AS13335
  - descrição CloudFlare, Inc.
  - localização Estados Unidos
  - ptr dolly.ns. **cloudflare.com**
- 2606:4700:50::adf5:3a62
  - rota 2606:4700:50::/44
  - bgp AS13335
  - descrição CloudFlare, Inc.
  - localização Estados Unidos
  - ptr dolly.ns. **cloudflare.com**

2803:f800:50::6ca2:c062
rota 2000::/3
bgp AS12874
descrição Cloudflare, Inc.
localização Costa Rica
2a06:98c1:50::ac40:2062
rota 2000::/3
bgp AS12874
descrição CloudFLARENET-EU

localização Reino Unido
108.162.192.98
quem é Cloudflare, Inc. (CLOUD14)
descrição CloudFlare, Inc.
localização São Francisco, Estados Unidos
ptr dolly.ns. **cloudflare.com**
172.64.32.98
quem é Cloudflare, Inc. (CLOUD14)
rota 172.64.0.0/16

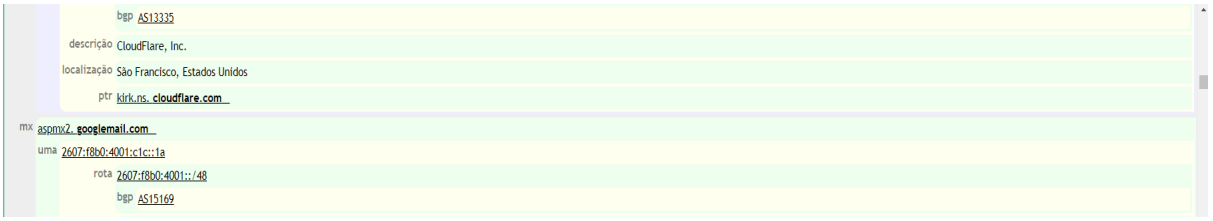
bgp AS13335
descrição CloudFlare, Inc.
localização São Francisco, Estados Unidos
173.245.58.98
quem é Cloudflare, Inc. (CLOUD14)
rota 173.245.58.0/24
bgp AS13335
descrição CloudFlare, Inc.
localização São Francisco, Estados Unidos

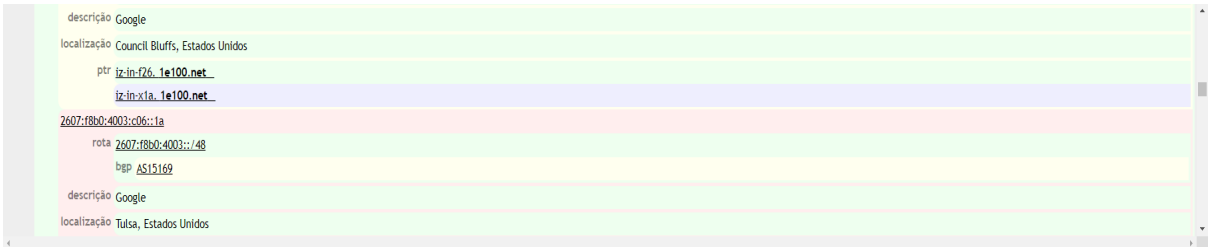
ptr dolly.ns. **cloudflare.com**
kirk.ns. **cloudflare.com**
uma 2400:cb00:2049:1::adf5:3bc0
rota 2400:cb00:2049::/48
bgp AS13335
descrição CloudFlare, Inc.
localização Estados Unidos
ptr kirk.ns. **cloudflare.com**
2606:4700:58::adf5:3bc0

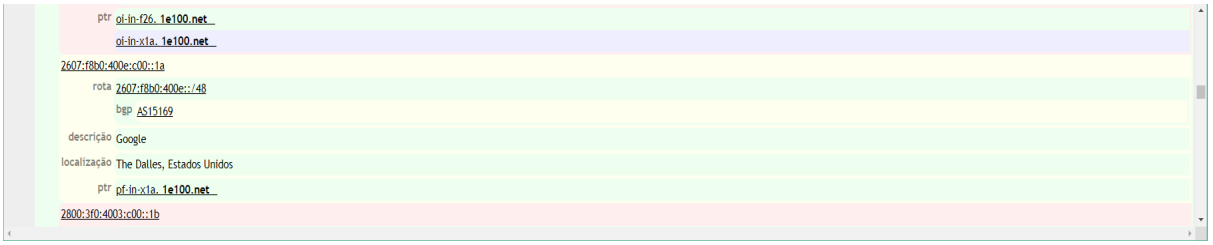
2606:4700:58::adf5:3bc0
rota 2606:4700:50::/44
bgp AS13335
descrição CloudFlare, Inc.
localização Estados Unidos
ptr kirk.ns. **cloudflare.com**
2803:f800:50::6ca2:c1c0
rota 2000::/3

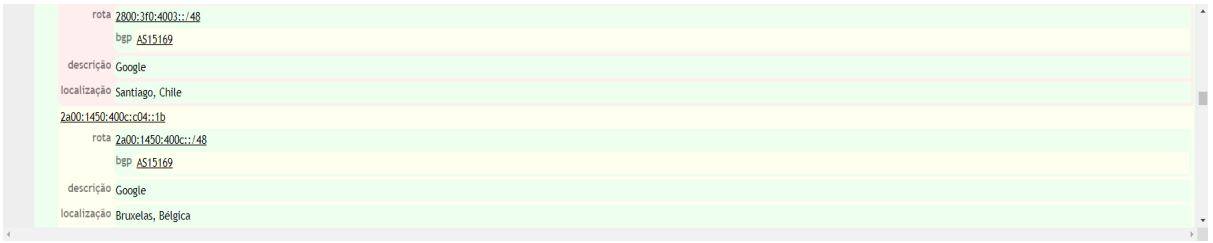
bgp AS12874
descrição CloudFLARENET-EU
localização Reino Unido
108.162.193.192
quem é Cloudflare, Inc. (CLOUD14)
descrição CloudFlare, Inc.
localização São Francisco, Estados Unidos
ptr kirk.ns. **cloudflare.com**

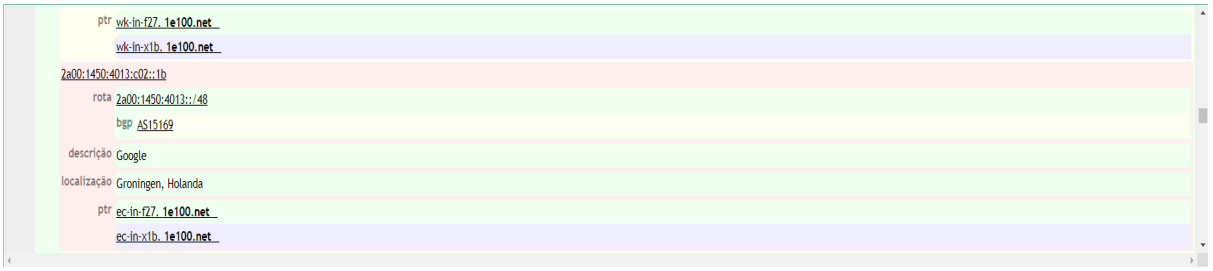
172.64.33.192
quem é Cloudflare, Inc. (CLOUD14)
rota 172.64.0.0/16
bgp AS13335
descrição CloudFlare, Inc.
localização São Francisco, Estados Unidos
173.245.59.192
quem é Cloudflare, Inc. (CLOUD14)
rota 173.245.59.0/24

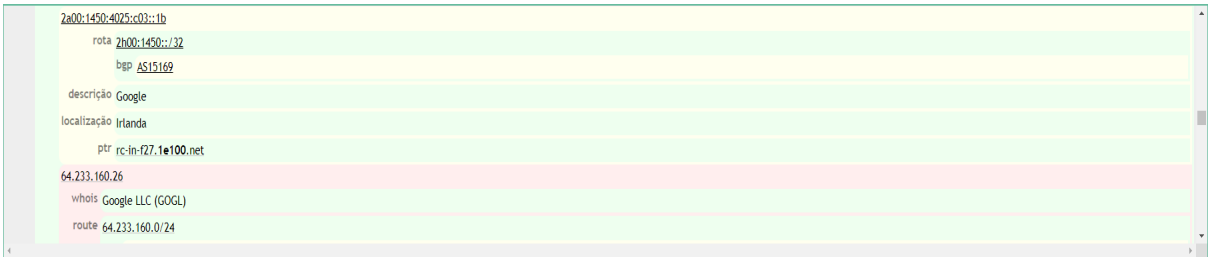

bgp AS13335
descrição CloudFlare, Inc.
localização São Francisco, Estados Unidos
ptr kirk.ns. cloudflare.com
mx aspmx2. googlemail.com
uma 2607:f8b0:4001:c1c::1a
rota 2607:f8b0:4001::/48
bgp AS15169

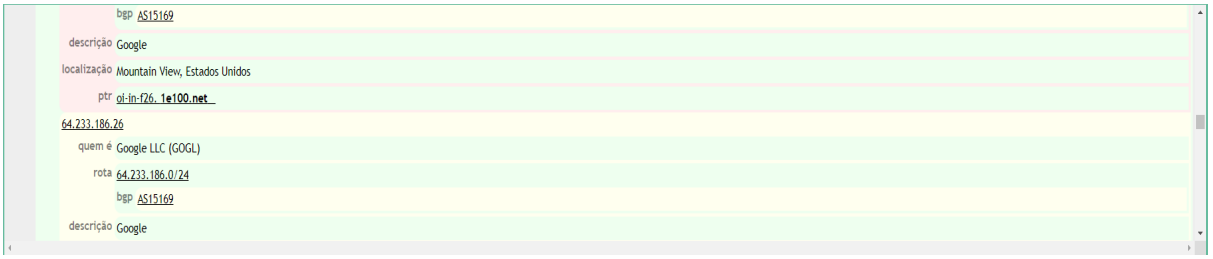

descrição Google
localização Council Bluffs, Estados Unidos
ptr iz-in-f26. 1e100.net
iz-in-x1a. 1e100.net
2607:f8b0:4003:c06::1a
rota 2607:f8b0:4003::/48
bgp AS15169
descrição Google
localização Tulsa, Estados Unidos

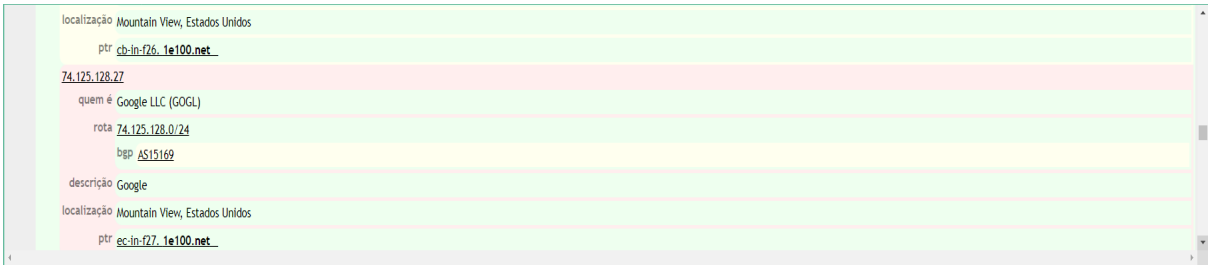

ptr oi-in-f26. 1e100.net
oi-in-x1a. 1e100.net
2607:f8b0:400e:c00::1a
rota 2607:f8b0:400e::/48
bgp AS15169
descrição Google
localização The Dalles, Estados Unidos
ptr pf-in-x1a. 1e100.net
2800:3f0:4003:c00::1b

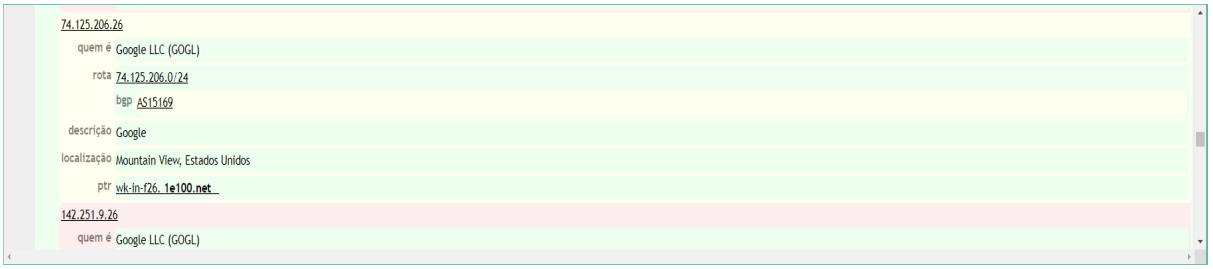

rota 2800:3f0:4003::/48
bgp AS15169
descrição Google
localização Santiago, Chile
2a00:1450:400c:c04::1b
rota 2a00:1450:400c::/48
bgp AS15169
descrição Google
localização Bruxelas, Bélgica

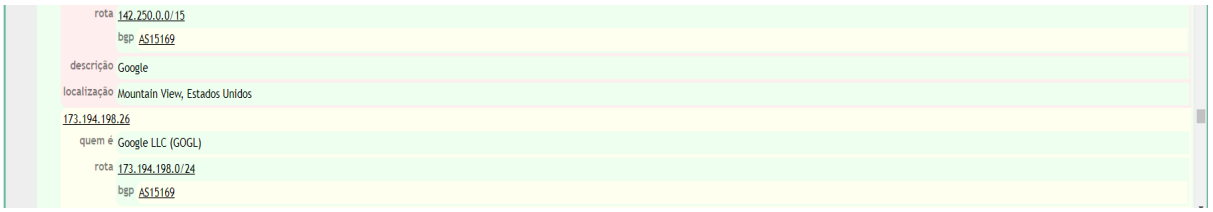

ptr wk-in-f27. 1e100.net
wk-in-x1b. 1e100.net
2a00:1450:4013:c02::1b
rota 2a00:1450:4013::/48
bgp AS15169
descrição Google
localização Groningen, Holanda
ptr ec-in-f27. 1e100.net
ec-in-x1b. 1e100.net

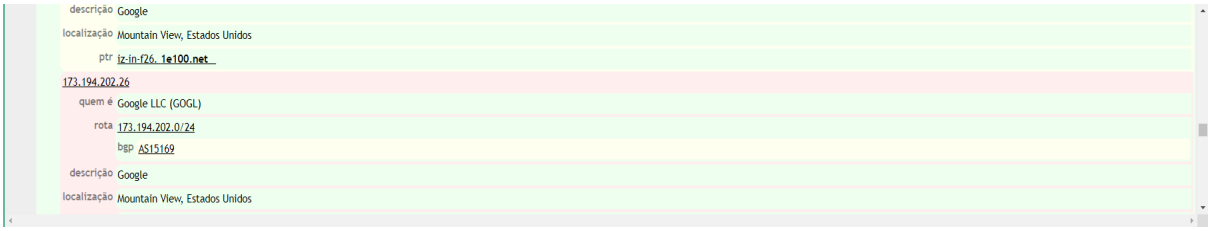

2a00:1450:4025:c03::1b
rota 2h00:1450::/32
bgp AS15169
descrição Google
localização Irlanda
ptr rc-in-f27.1e100.net
64.233.160.26
whois Google LLC (GOGL)
route 64.233.160.0/24

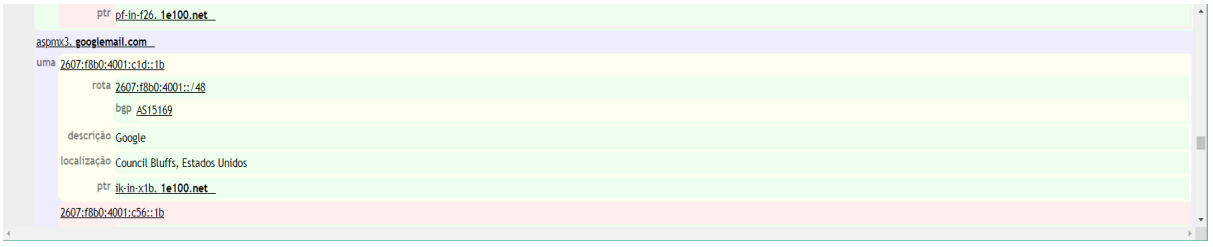

bgp AS15169
descrição Google
localização Mountain View, Estados Unidos
ptr oi-in-f26. 1e100.net
64.233.186.26
quem é Google LLC (GOGL)
rota 64.233.186.0/24
bgp AS15169
descrição Google

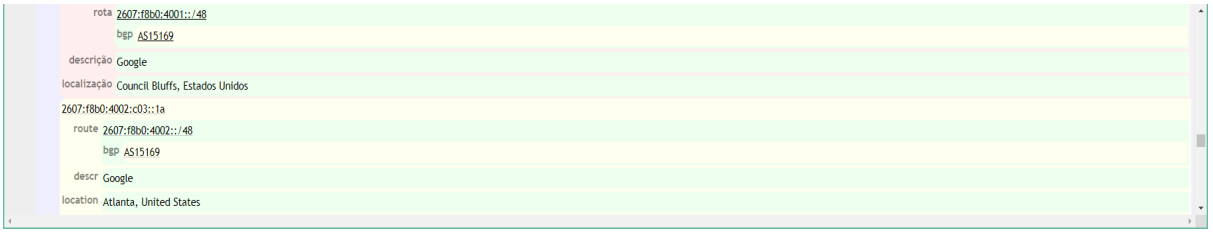

localização Mountain View, Estados Unidos
ptr cb-in-f26. 1e100.net
74.125.128.27
quem é Google LLC (GOGL)
rota 74.125.128.0/24
bgp AS15169
descrição Google
localização Mountain View, Estados Unidos
ptr ec-in-f27. 1e100.net

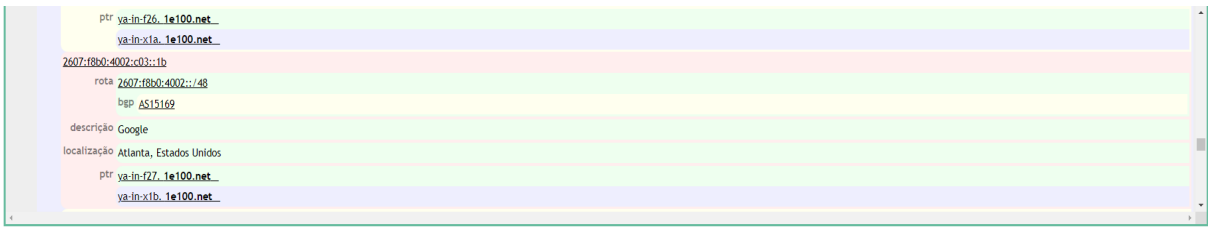

74.125.206.26
quem é Google LLC (GOGL)
rota 74.125.206.0/24
bgp AS15169
descrição Google
localização Mountain View, Estados Unidos
ptr wk-in-f26. 1e100.net
142.251.9.26
quem é Google LLC (GOGL)

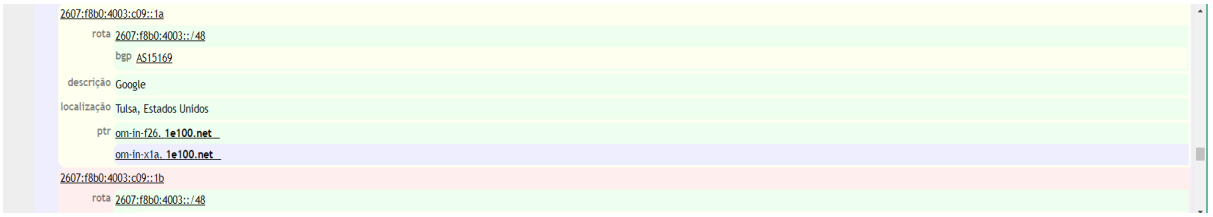

rota 142.250.0.0/15
bgp AS15169
descrição Google
localização Mountain View, Estados Unidos
173.194.198.26
quem é Google LLC (GOGL)
rota 173.194.198.0/24
bgp AS15169

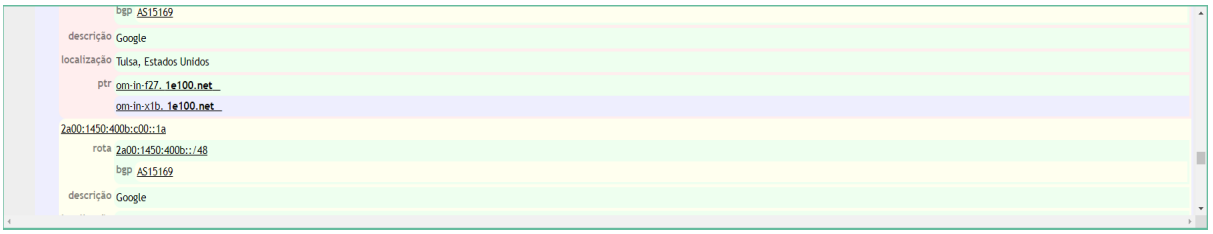

descrição Google
localização Mountain View, Estados Unidos
ptr iz-in-f26. 1e100.net
173.194.202.26
quem é Google LLC (GOGL)
rota 173.194.202.0/24
bgp AS15169
descrição Google
localização Mountain View, Estados Unidos

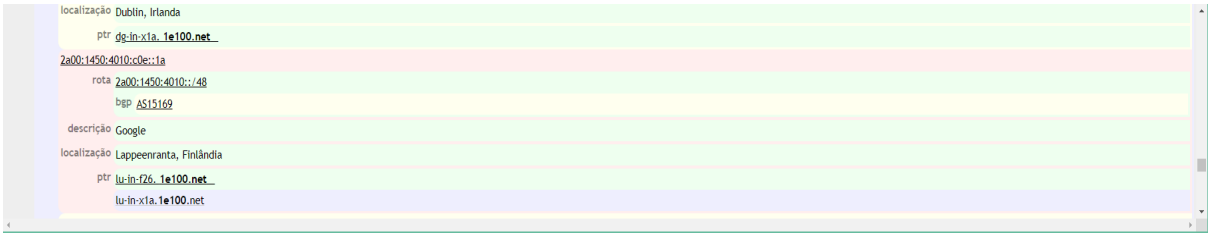

ptr pf-in-f26. 1e100.net
aspmx3. googlemail.com
uma 2607:f8b0:4001:c1d::1b
rota 2607:f8b0:4001::/48
bgp AS15169
descrição Google
localização Council Bluffs, Estados Unidos
ptr ik-in-x1b. 1e100.net
2607:f8b0:4001:c56::1b

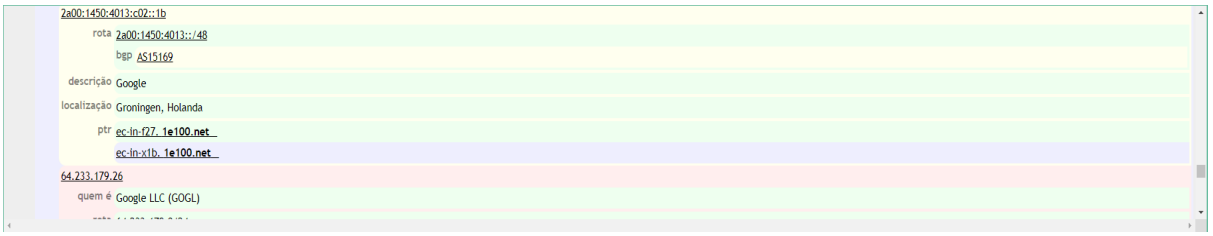

rota 2607:f8b0:4001::/48
bgp AS15169
descrição Google
localização Council Bluffs, Estados Unidos
2607:f8b0:4002:c03::1a
route 2607:f8b0:4002::/48
bgp AS15169
descr Google
location Atlanta, United States

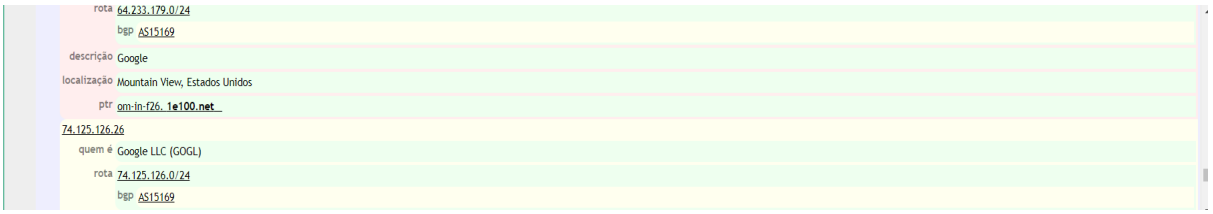

ptr va-in-f26. 1e100.net
va-in-x1a. 1e100.net
2607:f8b0:4002::c03::1b
rota 2607:f8b0:4002::/48
bgp AS15169
descrição Google
localização Atlanta, Estados Unidos
ptr va-in-f27. 1e100.net
va-in-x1b. 1e100.net

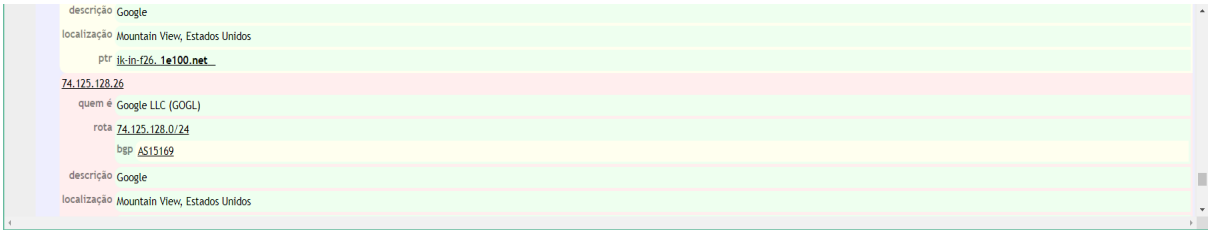

2607:f8b0:4003::c09::1a
rota 2607:f8b0:4003::/48
bgp AS15169
descrição Google
localização Tulsa, Estados Unidos
ptr om-in-f26. 1e100.net
om-in-x1a. 1e100.net
2607:f8b0:4003::c09::1b
rota 2607:f8b0:4003::/48


bgp AS15169
descrição Google
localização Tulsa, Estados Unidos
ptr om-in-f27. 1e100.net
om-in-x1b. 1e100.net
2a00:1450:400b::c00::1a
rota 2a00:1450:400b::/48
bgp AS15169
descrição Google


localização Dublin, Irlanda
ptr dg-in-x1a. 1e100.net
2a00:1450:4010:c0e::1a
rota 2a00:1450:4010::/48
bgp AS15169
descrição Google
localização Lappeenranta, Finlândia
ptr lu-in-f26. 1e100.net
lu-in-x1a.1e100.net


2a00:1450:4013::c02::1b
rota 2a00:1450:4013::/48
bgp AS15169
descrição Google
localização Groningen, Holanda
ptr ec-in-f27. 1e100.net
ec-in-x1b. 1e100.net
64.233.179.26
quem é Google LLC (GOGL)


rota 64.233.179.0/24
bgp AS15169
descrição Google
localização Mountain View, Estados Unidos
ptr om-in-f26. 1e100.net
74.125.126.26
quem é Google LLC (GOGL)
rota 74.125.126.0/24
bgp AS15169


descrição Google
localização Mountain View, Estados Unidos
ptr ik-in-f26. 1e100.net
74.125.128.26
quem é Google LLC (GOGL)
rota 74.125.128.0/24
bgp AS15169
descrição Google
localização Mountain View, Estados Unidos

ptr	ec-in-f26. 1e100.net

74.125.131.26

quem é	Google LLC (GOGL)
rota	74.125.131.0/24
bgp	AS15169
descrição	Google
localização	Mountain View, Estados Unidos
ptr	lu-in-f26. 1e100.net

142.250.152.26

quem é	Google LLC (GOGL)
rota	142.250.0.0/15
bgp	AS15169
descrição	Google
localização	Mountain View, Estados Unidos
ptr	ia-in-f26. 1e100.net

173.194.219.26

quem é	Google LLC (GOGL)
rota	173.194.219.0/24
bgp	AS15169
descrição	Google
localização	Mountain View, Estados Unidos
ptr	ya-in-f26. 1e100.net

209.85.202.26

quem é	Google LLC (GOGL)
rota	
descrição	GBLX-US-BGP
localização	Estados Unidos
ptr	dg-in-f26. 1e100.net

acima com

SEO

Informações sobre otimização de mecanismos de pesquisa

backblaze.com dados de SEO

SEMrush

Nothing found here, sorry

Em vez disso, verifique semrush .

ALEXA

Classifique e pesquise porcentagens do Alexa.

Classificação Global de backblaze.com

Tendência de classificação global diária de backblaze.com

Visitas de pesquisa de backblaze.com em porcentagem

Visitas de pesquisa (porcentagem) de backblaze.com

Fonte: Alexa

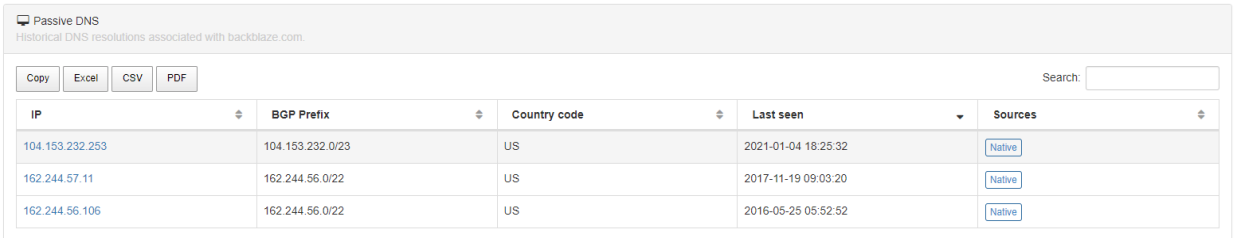
AMEAÇA

Informações sobre ameaças, como vírus, etc.

Informações

modelo	dados
Data de criação	Indefinido
Data atualizada	Indefinido
Data de validade	Indefinido
Informações do Registrante	Indefinido
Informação de pagamento	Indefinido
Informações técnicas	Indefinido
Informações do administrador	Indefinido
registrador	Indefinido

Fonte: Threatminer

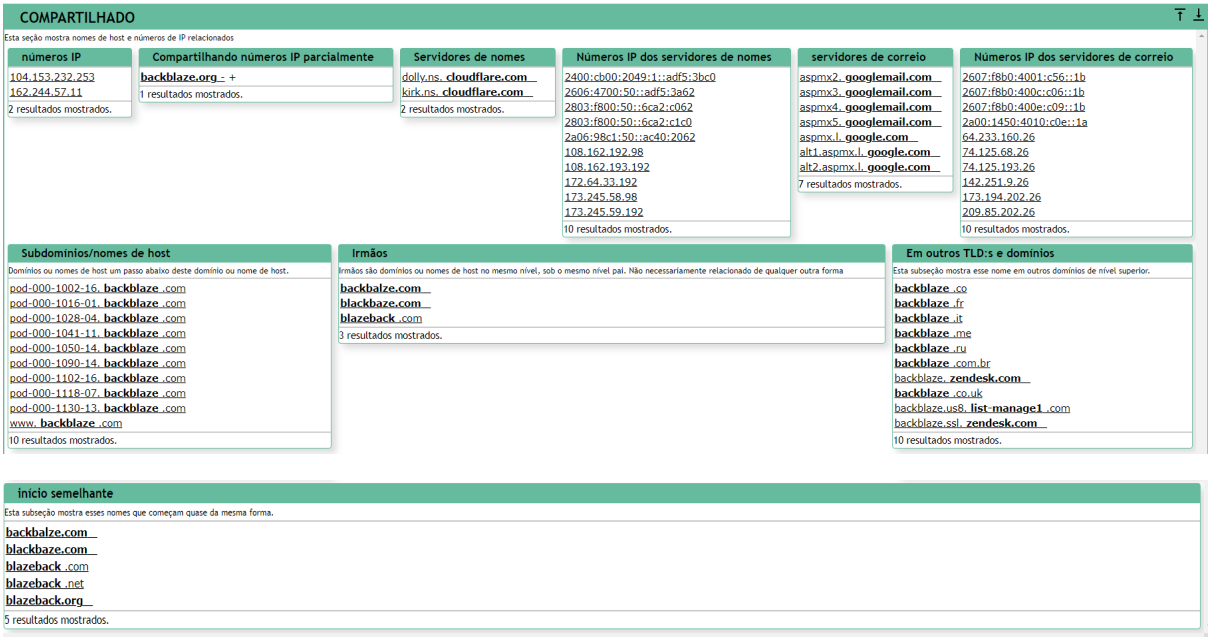


Passive DNS

Historical DNS resolutions associated with backblaze.com

Copy | Excel | CSV | PDF | Search:

IP	BGP Prefix	Country code	Last seen	Sources
104.153.232.253	104.153.232.0/23	US	2021-01-04 18:25:32	Native
162.244.57.11	162.244.56.0/22	US	2017-11-19 09:03:20	Native
162.244.56.106	162.244.56.0/22	US	2016-05-25 05:52:52	Native



COMPARTILHADO

Esta seção mostra nomes de host e números de IP relacionados

números IP
104.153.232.253
162.244.57.11
2 resultados mostrados.

Compartilhando números IP parcialmente
backblaze.org - +
1 resultados mostrados.

Servidores de nomes
dolly.ns. cloudflare.com
kirk.ns. cloudflare.com
2 resultados mostrados.

Números IP dos servidores de nomes
2400:cb00:2049:1::adf5:3bc0
2606:4700:50::adf5:3a62
2803:f800:50::6ca2:c062
2803:f800:50::6ca2:c1c0
2a06:98c1:50::ac40:2062
108.162.192.98
108.162.193.192
172.64.33.192
173.245.58.98
173.245.59.192
10 resultados mostrados.

servidores de correio
aspmx2. googlemail.com
aspmx3. googlemail.com
aspmx4. googlemail.com
aspmx5. googlemail.com
aspmx.l. google.com
alt1.aspmx.l. google.com
alt2.aspmx.l. google.com
7 resultados mostrados.

Números IP dos servidores de correio
2607:f8b0:4001:c56::1b
2607:f8b0:400c:c06::1b
2607:f8b0:400e:c09::1b
2a00:1450:4010:c0e::1a
64.233.160.26
74.125.68.26
74.125.193.26
142.251.9.26
173.194.202.26
209.85.202.26
10 resultados mostrados.

Subdomínios/nomes de host
Domínios ou nomes de host um passo abaixo deste domínio ou nome de host.
pod-000-1002-16. backblaze .com
pod-000-1016-01. backblaze .com
pod-000-1028-04. backblaze .com
pod-000-1041-11. backblaze .com
pod-000-1050-14. backblaze .com
pod-000-1090-14. backblaze .com
pod-000-1102-16. backblaze .com
pod-000-1118-07. backblaze .com
pod-000-1130-13. backblaze .com
www. backblaze .com
10 resultados mostrados.

Irmãos
Irmãos são domínios ou nomes de host no mesmo nível, sob o mesmo nível pai. Não necessariamente relacionado de qualquer outra forma
backbalze.com
blackbaze.com
blazeback .com
3 resultados mostrados.

Em outros TLD:s e domínios
Esta subseção mostra esse nome em outros domínios de nível superior.
backblaze .co
backblaze .fr
backblaze .it
backblaze .me
backblaze .ru
backblaze .com.br
backblaze. zendesk.com
backblaze .co.uk
backblaze.us8. list-manage1 .com
backblaze.ssl. zendesk.com
10 resultados mostrados.

início semelhante
Esta subseção mostra esses nomes que começam quase da mesma forma.
backbalze.com
blackbaze.com
blazeback .com
blazeback .net
blazeback.org
5 resultados mostrados.

4. DETALHAMENTO DOS SOFTWARES INSTALADOS

- **Análise e Rastreamento**

Hotjar	Hubspot	Visual Website Optimizer	Google Optimize 360	Google Analytics	LinkedIn Insights

Facebook Domain Insights	Facebook Pixel	Facebook Signal	Twitter Analytics	Twitter Conversion Tracking	Twitter Website Universal Tag
Bing Universal Event Tracking	Global Site Tag	Google Conversion Tracking	Google Conversion Linker	DoubleClick Floodlight	

- **Widgets**

HubSpot Messages	Apple Whitelist	OneTrust	Optanon	HubSpot Conversations	Zoom Video Conferencing
Cloudflare Bot Manager	Google Font API	Google Tag Manager	 Responsive Lightbox	Wordpress Plugins	Disqus Comment System for Wordpress
Sitelinks Search Box	GDPR Consent Management Platform	US Privacy User Signal Mechanism			

- **eCommerce**

Woo Commerce

- **Frameworks**

Bug Bounty	ContactPoint Schema	Postal Address Schema	Organization Schema

- **Rede de Entrega de Conteúdo**

GStatic Google Static Content	Akamai	OSS CDN	Cloudflare	CDN JS

- **Dispositivos Móveis**

Apple Mobile Web Clips Icon	Viewport Meta	IPhone / Mobile Compatible

- **Forma de Pagamento**

Euro

- **Mídia de Áudio e Vídeo**

Zoom	YouTube

- **Sistema de Gerenciamento de Conteúdo**

My Salesforce	Atlassian Cloud	Postman	WordPress

- **Bibliotecas e Funções JavaScript**

Facebook for Websites	Facebook SDK	Modernizr	Images Loaded	Respond	HTML5 History API
React	Emotion				

- **Publicidade**

Double Click.Net	AdRoll	Facebook Custom Audiences	Twitter Ads	Google Remarketing	Google Floodlight Counter
LinkedIn Ads	Consent Management Platform API v 2.0				

- **Link Verificado**

Facebook	LinkedIn	Twitter	Instagram

- **Provedores de Hospedagem de E-mail**

Sendgrid	Zendesk	Postmark	Google Apps for Business	SPF	DMARC

- **Nome do Servidor**

3 to 9 ccTLD Redirects	Amazon Route 53	Cloudflare DNS

- **Provedores de Hospedagem na Web**

Many Subdomains	Cloudflare Hosting

- **Certificados SSL**

SSL by Default	Cloudflare SSL	HSTS

- **Servidores Web**

nginx

- **Sistemas Operacionais e Servidores**

IPv6

- **Técnicas de Distribuição**

Really Simple DIscovery	RSS	Live Writer Support

- **CDN Verificado**

Cloudflare CDN

- **Rede de Entrega de Conteúdo**

Content Delivery Network

- **Registro de Webmaster**

Google Webmaster

5. METODOLOGIA

As etapas a seguir, foram conduzidas para fornecer uma avaliação dos riscos com base na norma ABNT NBR ISO/IEC 27005:2011 com intuito de determinar eventos que possam causar uma perda potencial e auxiliar na adequação dos controles de segurança do ambiente testado:

• **Identificação de Ameaças**: identificar ameaças e potenciais de comprometer ativos (como informações, processos e sistemas);
• **Identificação de Vulnerabilidade**: analisar vulnerabilidades que podem ser exploradas por ameaças para comprometer os ativos;
• **Determinação do nível das Vulnerabilidades**: A análise das vulnerabilidades é baseada nas consequências e na probabilidade de um cenário de incidente e suas consequências.
• **Avaliação das consequências**: determinar medidas apropriadas através do entendimento das vulnerabilidades por meio análise dos riscos para a tomada de decisões sobre ações futuras.

5.1 Identificação de Ameaças

A primeira fase da avaliação concentrou-se na coleta, análise e estruturação de informações sobre os itens do escopo, utilizando principalmente técnicas de análise passiva, além de normas, fontes públicas como sites, blogs e mecanismos de pesquisa, que foram consultadas para obtenção e reconhecimento de informações sobre o ambiente testado. Isso é feito para coletar informações necessárias para conduzir as demais fases dos testes. Vale ressaltar que uma ameaça pode surgir de dentro ou de fora da organização e isso significa que nenhuma ameaça será ignorada. Dessa forma, as ameaças foram identificadas genericamente e classificadas de acordo com a sua gravidade percebida.

5.2 Identificação das Vulnerabilidades

Testes automatizados e manuais foram combinados para confirmar a maioria das vulnerabilidades potenciais. Pois, uma vulnerabilidade que não tem uma ameaça correspondente pode não requerer a implementação de um controle no presente momento, mas convém que ela seja reconhecida como tal e monitorada, no caso de haver mudanças. Sendo assim, ao testar de diferentes formas os aspectos críticos, as falhas de segurança que não foram descobertas por determinado método puderam ser encontradas e avaliadas conforme o CVSS (Common Vulnerability Scoring System).

5.3 Determinação do nível das Vulnerabilidades

A análise das vulnerabilidades designa valores para a probabilidade e para as consequências de um risco. Esses valores (com base CVSS) foram atribuídos aos resultados das análises manuais e automatizadas verificando quanto à sua integridade e razoabilidade a fim de se diminuir o risco de vulnerabilidades não identificadas (falsos negativos) para um nível aceitável. Com isso, as descobertas foram avaliadas e reavaliadas individualmente para verificar se elas representavam, de fato, vulnerabilidades.

5.4 Avaliação das consequências

O relatório foi construído com base no escopo que a empresa BackBlaze disponibilizou no site da bugcrowd.com. Para as futuras decisões a serem tomadas convém que as consequências, a probabilidade e o grau de confiança na identificação e determinação do nível das vulnerabilidades também sejam considerados. Por fim, é importante ressaltar que foi seguido à risca o que foi solicitado e todo o progresso geral com informações sobre a realização dos testes juntamente com os resultados da avaliação foram aqui documentados e serão entregues na forma deste relatório.

5.5 Ferramentas Utilizadas
As ferramentas mencionadas abaixo foram executadas no Kali Linux Versão 2022.3.

● **Spiderfoot**: funciona de maneira parecida com o DNSdumpster.com, pois sendo uma ferramenta de análise não invasiva, ela traz o máximo possível de informações que não se encontra com muita facilidade, como emails, endereços de IP, nomes de domínio, subdomínios, números de telefone, nomes de usuários, dentre outros, tudo relacionado à informação inserida no campo de pesquisa da ferramenta;

● **DNSdumpster.com**: é uma ferramenta GRATUITA de pesquisa de domínio que pode descobrir hosts relacionados a um domínio. E encontrar hosts visíveis da perspectiva dos invasores é uma parte importante do processo de avaliação de segurança;

● **Haveibeenpwned.com**: é uma ferramenta gratuita e online que nos revela se um endereço de email ou número de telefone foi vazado em algum site que estava cadastrado;

● **NMAP**: é uma ferramenta de código aberto para exploração de rede e auditoria de segurança. Ela foi desenhada para escanear rapidamente redes amplas, embora também funcione muito bem contra hosts individuais. O Nmap utiliza pacotes IP em estado bruto (raw) de maneira inovadora para determinar quais hosts estão disponíveis na rede, quais serviços (nome da aplicação e versão) os hosts oferecem, quais sistemas operacionais (e versões de SO) eles estão executando, que tipos de filtro de pacotes/firewalls estão em uso, e dezenas de outras características;

● **BuiltWith**: é uma ferramenta de criação de perfil de website, geração de leads, análise competitiva e inteligência de negócios que fornece adoção de tecnologia, dados de comércio eletrônico e análise de uso para a internet.O rastreamento da tecnologia BuiltWith inclui widgets, análises, estruturas, sistemas de gerenciamento de conteúdo, anunciantes, redes de distribuição de conteúdo, padrões da web e servidores da web.

● **whois.domaintools.com:** utilizado para buscar informações sobre o site, como: domínio, subdomínios.

● **toolbar.netcraft.com**: utilizado para buscar informações sobre a tecnologia utilizada no site.

● **robtex.com**: utilizado para encontrar todas as informações do site, como: DNS.

6. EQUIPE TÉCNICA

NOME	RESPONSABILIDADE	CONTATO
Luís Guilherme Rocha Ribeiro	Reconhecimento do ambiente, teste, elaboração de conceitos e produção do relatório.	guigas0608@gmail.com

Edson Lara Bastos	Reconhecimento do ambiente, teste, elaboração de conceitos e produção do relatório.	mystudentacount.edson@gmail.com

7. CRONOGRAMA DE ATIVIDADES

ATIVIDADE	**DATA DA REALIZAÇÃO**
Pesquisas e reconhecimento de sistemas computacionais envolvidos no escopo.	26 de novembro de 2022
Provas de conceito e conclusão dos testes.	28 de novembro de 2022
Avaliação dos riscos e esboço do relatório	28 de novembro de 2022
Conclusão e revisão final do relatório	30 de novembro de 2022

8. NÍVEIS DE CRITICIDADE

Para categorizar o impacto e a exploração de vulnerabilidades, os níveis de criticidade usados na seção “Vulnerabilidades Encontradas” estão de acordo com a Versão 3 do Common Vulnerability Scoring System (CVSS v3) do NIST, o qual utiliza a pontuação básica composta pelo tipo de acesso, a complexidade de acesso e o nível de autenticação exigido para explorar uma determinada vulnerabilidade, bem como o impacto relacionado à confidencialidade, integridade e disponibilidade. A pontuação aplicada às vulnerabilidades varia de 0 a 10 pontos e é normalizada categorizando-as em níveis críticos, altos, médios e baixos de criticidade.

● Vetor de Acesso (AV): descreve a fonte necessária de ataque para explorar uma vulnerabilidade, cujos valores possíveis são Local (L), Rede Adjacente (A) ou Rede (N);

● Complexidade do Acesso (AC): está relacionado à complexidade das condições que precisam estar em vigor para uma exploração bem-sucedida. Os valores possíveis são Alto (H), Médio (M) e Baixo (L);

● Autenticação (AU): refere-se aos níveis de autenticação que um invasor precisa transmitir para explorar uma vulnerabilidade. Os valores possíveis são: Requer Várias Instâncias (M), Requer Instância Única (S) e Nenhum Requerido (N);

● Confidencialidade (C), Integridade (I), Disponibilidade (A): quando há impacto na confidencialidade, integridade ou disponibilidade, e cujos possíveis valores são Nenhum (N), Parcial (P) e Completo (C).

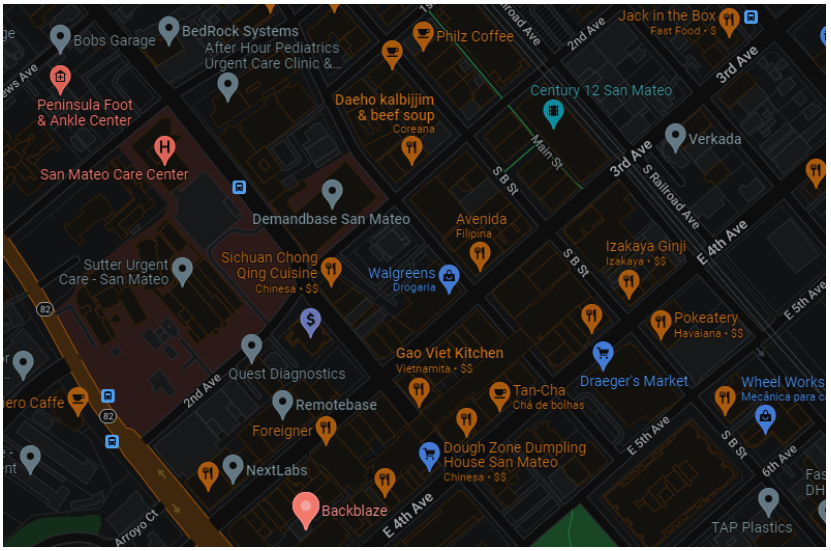
Diante do exposto, os níveis de criticidade definidos podem ser visualizados na Tabela 1, a seguir, de acordo com o resultado da soma de seus fatores de risco, juntamente com seu respectivo significado. Tais níveis foram utilizados para representar o risco e a criticidade calculados para cada uma das vulnerabilidades que foram identificadas.

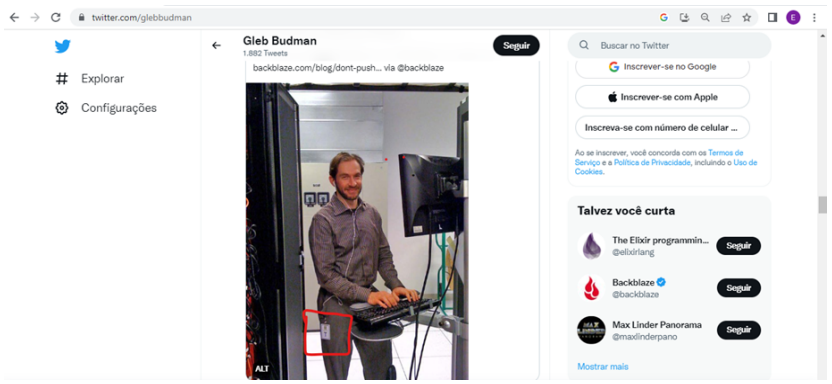
CRITICIDADE	DESCRIÇÃO

Crítica	● Pontuação Base do CVSS: 9 a 10 pontos; ● Exploração trivial; ● Perda de confidencialidade, integridade e disponibilidade. **A remediação imediata é crítica para os negócios.**
Alta	● Pontuação Base do CVSS: de 6 a 8.9 pontos; ● Exploração quase trivial; ● Perda ou de confidencialidade, ou de integridade ou de disponibilidade. **A remediação é crítica para os negócios.**
Média	● Pontuação Base do CVSS: de 4 a 6.9 pontos; ● Exploração possível e comum, mas requer habilidades; ● Sério impacto na confidencialidade, integridade e disponibilidade. **Ações corretivas são exigidas dentro de um prazo razoável.**
Baixa	● Pontuação Base do CVSS: de 0.1 a 3.9 pontos; ● Exploração possível, mas difícil e improvável; ● Impacto mensurável na confidencialidade, disponibilidade. **Ações corretivas são recomendadas.**
Informativa	Nenhuma vulnerabilidade real foi identificada, mas há informações que podem ser relevantes para melhorar a segurança do ambiente.

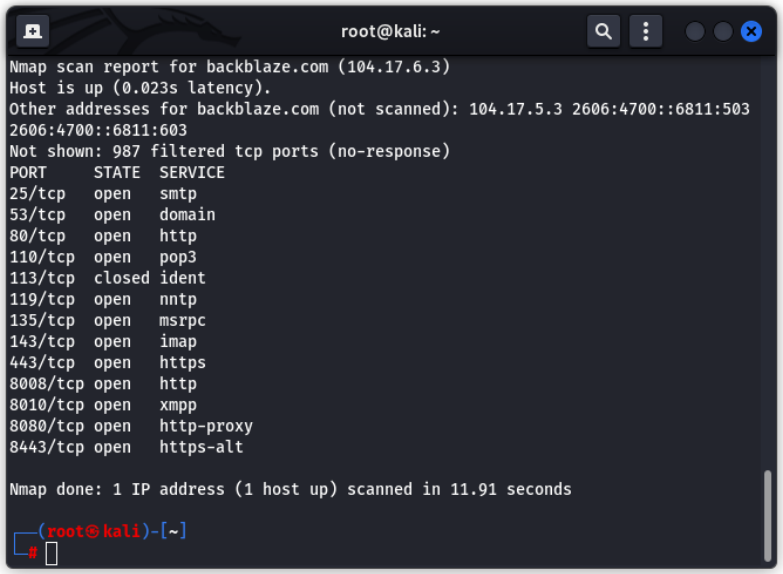
9. VULNERABILIDADES ENCONTRADAS

ID de Vulnerabilidade 01	Engenharia Social
Criticidade	Informativo
Título	Vulnerabilidade Via Google Maps (Street View)
Descrição	Os arredores do local onde se encontra o escritório central da empresa, estão repletos de restaurantes e locais onde há possibilidade de encontros públicos, o que pode ser perigoso por permitir oportunidades de engenharia social.

Evidência	  
Recomendação	Promover palestras entre os funcionários para que eles entendam os perigos relacionados à engenharia social e que assim evitem conversas potencialmente reveladoras sobre informações da empresa em locais públicos.

ID de Vulnerabilidade 01	Engenharia Social
Criticidade	Informativo
Título	Vulnerabilidade via Redes Sociais
Descrição	Uma das principais formas de conseguir informações necessárias para ter acesso à uma empresa, é através de fotos postadas por funcionários em suas redes sociais, utilizando o crachá da empresa.
Evidência	
Recomendação	Orientar os funcionários sobre o cuidado com as redes sociais, não utilizando o crachá em locais públicos, não postando fotos com o crachá ou que contenham alguma informação interna e sigilosa da empresa, e removendo as fotos que já tenham sido postadas antes das orientações.

ID da Vulnerabilidade 02	Verificação de Portas
Criticidade	Informativo
Título	Identificação de portas abertas
Descrição	As portas 25, 53, 80, 110, 119, 135, 143, 443, 8008, 8018, 8080 e 8443 estão abertas e sem filtro do firewall no servidor rodando alguns serviços
URL afetado	backblaze.com

Evidência	
Recomendação	Recomenda-se que proteja seu alvo com um filtro de IP.

ID da Vulnerabilidade 03	E-mails no site
Criticidade	Informativo
Título	Emails com dados vazados em plataformas online
Descrição	Alguns emails relacionados à BackBlaze tiveram seus dados vazados em algumas plataformas que sofreram de Data Breach. Os e-mails afetados foram: helpme@backblaze.com abuse@cloudflare.com abuse@hubspot.com techops@hubspot.com romulobil@gmail.com rir@cloudflare.com product-security@apple.com noc@cloudflare.com network-abuse@google.com kbaker@hubspot.com jross@carsim.com hellointernet@cgpgrey.com atp@marco.org arin-contact@google.com albuquerque@ufpa.br salescontact@backblaze.com productfeedback@backblaze.com affiliatehelp@backblaze.com partnercontact@backblaze.com

	sponsorships@backblaze.com press@backblaze.com legal@backblaze.com reportphising@backblaze.com jobscontact@backblaze.com

techops@hubspot.com pwned?

Oh no — pwned!

Pwned in 1 data breach and found no pastes (subscribe to search sensitive breaches)

romulobil@gmail.com pwned?

Oh no — pwned!

Pwned in 8 data breaches and found no pastes (subscribe to search sensitive breaches)

rir@cloudflare.com pwned?

Oh no — pwned!

Not pwned in any data breaches, but found 14 pastes (subscribe to search sensitive breaches)

product-security@apple.com pwned?

Oh no — pwned!

Pwned in 4 data breaches and found 10 pastes (subscribe to search sensitive breaches)

noc@cloudflare.com pwned?

Oh no — pwned!

Pwned in 5 data breaches and found 29 pastes (subscribe to search sensitive breaches)

network-abuse@google.com pwned?

Oh no — pwned!

Not pwned in any data breaches, but found 7 pastes (subscribe to search sensitive breaches)

kbaker@hubspot.com pwned?

Oh no — pwned!

Pwned in 8 data breaches and found no pastes (subscribe to search sensitive breaches)

jross@carsim.com pwned?

Oh no — pwned!

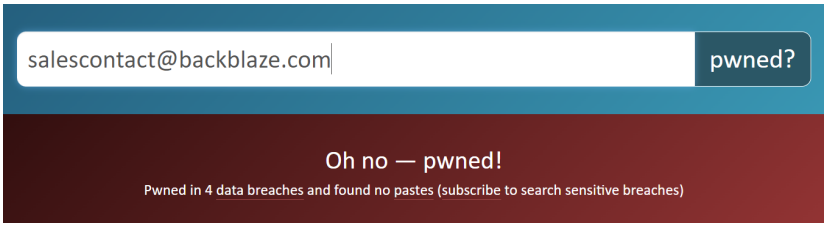
Pwned in 5 data breaches and found no pastes (subscribe to search sensitive breaches)

hellointernet@cgpgrey.com pwned?

Oh no — pwned!

Pwned in 2 data breaches and found no pastes (subscribe to search sensitive breaches)

	 atp@marco.org pwned? Oh no — pwned! Pwned in 1 data breach and found no pastes (subscribe to search sensitive breaches) arin-contact@google.com pwned? Oh no — pwned! Pwned in 6 data breaches and found 24 pastes (subscribe to search sensitive breaches) albuquerque@ufpa.br pwned? Oh no — pwned! Not pwned in any data breaches, but found 1 paste (subscribe to search sensitive breaches) abuse@hubspot.com pwned? Oh no — pwned! Not pwned in any data breaches, but found 1 paste (subscribe to search sensitive breaches) abuse@cloudflare.com pwned? Oh não - pwned! Pwned em 12 violações de dados e encontrou 35 pastas (inscreva -se para pesquisar violações confidenciais) helpme@backblaze.com pwned? Oh no — pwned! Pwned in 5 data breaches and found no pastes (subscribe to search sensitive breaches) partnercontact@backblaze.com pwned? Oh no — pwned! Pwned in 7 data breaches and found no pastes (subscribe to search sensitive breaches) affiliatehelp@backblaze.com pwned? Oh no — pwned! Pwned in 2 data breaches and found no pastes (subscribe to search sensitive breaches)



Anti Public Combo List (unverified): In December 2016, a huge list of email address and password pairs appeared in a "combo list" referred to as "Anti Public". The list contained 458 million unique email addresses, many with multiple different passwords hacked from various online systems. The list was broadly circulated and used for "credential stuffing", that is attackers employ it in an attempt to identify other online systems where the account owner had reused their password. For detailed background on this incident, read Password reuse, credential stuffing and another billion records in Have I Been Pwned.

Compromised data: Email addresses, Passwords

Apollo: In July 2018, the sales engagement startup Apollo left a database containing billions of data points publicly exposed without a password. The data was discovered by security researcher Vinny Troia who subsequently sent a subset of the data containing 126 million unique email addresses to Have I Been Pwned. The data left exposed by Apollo was used in their "revenue acceleration platform" and included personal information such as names and email addresses as well as professional information including places of employment, the roles people hold and where they're located. Apollo stressed that the exposed data did not include sensitive information such as passwords, social security numbers or financial data. The Apollo website has a contact form for those looking to get in touch with the organisation.

Compromised data: Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Salutations, Social media profiles

Covve: In February 2020, a massive trove of personal information referred to as "db8151dd" was provided to HIBP after being found left exposed on a publicly facing Elasticsearch server. Later identified as originating from the Covve contacts app, the exposed data included extensive personal information and interactions between Covve users and their contacts. The data was provided to HIBP by dehashed.com.

Compromised data: Email addresses, Job titles, Names, Phone numbers, Physical addresses, Social media profiles

Onliner Spambot (spam list): In August 2017, a spambot by the name of Onliner Spambot was identified by security researcher Benkow moɈuƎq. The malicious software contained a server-based component located on an IP address in the Netherlands which exposed a large number of files containing personal information. In total, there were 711 million unique email addresses, many of which were also accompanied by corresponding passwords. A full write-up on what data was found is in the blog post titled Inside the Massive 711 Million Record Onliner Spambot Dump.

Compromised data: Email addresses, Passwords

Verifications.io: In February 2019, the email address validation service verifications.io suffered a data breach. Discovered by Bob Diachenko and Vinny Troia, the breach was due to the data being stored in a MongoDB instance left publicly facing without a password and resulted in 763 million unique email addresses being exposed. Many records within the data also included additional personal attributes such as names, phone numbers, IP addresses, dates of birth and genders. No passwords were included in the data. The Verifications.io website went offline during the disclosure process, although an archived copy remains viewable.

Compromised data: Dates of birth, Email addresses, Employers, Genders, Geographic locations, IP addresses, Job titles, Names, Phone numbers, Physical addresses

MyHeritage : Em outubro de 2017, o site de genealogia MyHeritage sofreu uma violação de dados . O incidente foi relatado 7 meses depois, depois que um pesquisador de segurança descobriu os dados e contatou o MyHeritage. No total, mais de 92 milhões de registros de clientes foram expostos e incluíam endereços de e-mail e hashes de senha SHA-1 salgados. Em 2019, os dados apareceram listados para venda em um mercado da dark web (juntamente com várias outras grandes violações) e, posteriormente, começaram a circular de forma mais ampla. Os dados foram fornecidos ao HIBP por uma fonte que solicitou que fossem atribuídos a "BenjaminBlue@exploit.im".

Dados comprometidos: endereços de e-mail, senhas

NemoWeb : Em setembro de 2016, quase 21 GB de dados do site francês usados para "meios de troca padronizados e descentralizados para a publicação de artigos de grupos de notícias" NemoWeb vazaram do que parece ter sido um Mongo DB desprotegido. Os dados consistiam em um grande volume de e-mails enviados ao serviço e incluíam quase 3,5 milhões de endereços únicos, embora muitos deles gerados automaticamente. Várias tentativas foram feitas para entrar em contato com os operadores do NemoWeb, mas nenhuma resposta foi recebida.

Dados comprometidos: endereços de e-mail, nomes

OGUsers (violação de 2019) : em maio de 2019, o fórum de sequestro de contas e troca de SIM OGusers sofreu uma violação de dados . A violação expôs um backup de banco de dados de dezembro de 2018, publicado em um fórum de hackers rival. Havia 161 mil endereços de e-mail exclusivos espalhados por 113 mil usuários do fórum e outras tabelas no banco de dados. Os dados expostos também incluíam nomes de usuários, endereços IP, mensagens privadas e senhas armazenadas como hashes MD5 salgados.

Dados comprometidos: endereços de e-mail, endereços IP, senhas, mensagens privadas, nomes de usuário

OGUsers (violação de 2020) : em abril de 2020, o fórum de sequestro de contas e troca de SIM OGUsers sofreu sua segunda violação de dados em menos de um ano . Assim como na violação anterior, os dados expostos incluíam endereços de e-mail e IP, nomes de usuário, mensagens privadas e senhas armazenadas como hashes MD5 salgados. Um total de 263 mil endereços de e-mail em contas de usuários e outras tabelas foram postados em um fórum de hackers rival.

Dados comprometidos: endereços de e-mail, endereços IP, senhas, mensagens privadas, nomes de usuário

OGUsers (violação de 2021) : em abril de 2021, o fórum de sequestro de conta e troca de SIM OGusers sofreu uma violação de dados , a quarta desde dezembro de 2018. A violação foi posteriormente vendida em um fórum de hackers rival e continha nomes de usuário, e-mail, endereços IP e senhas armazenados como hashes MD5 salgados ou argon2. Um total de 348 mil endereços de e-mail exclusivos apareceram na violação.

Dados comprometidos: endereços de e-mail, endereços IP, senhas, nomes de usuário

Staminus : Em março de 2016, o serviço de proteção DDoS Staminus foi "hackeado massivamente" , resultando em uma interrupção de mais de 20 horas e na divulgação de credenciais do cliente (com hashes MD5 sem sal), tíquetes de suporte, números de cartão de crédito e outros dados confidenciais. 27 mil endereços de e-mail exclusivos foram encontrados nos dados que foram posteriormente divulgados ao público. Staminus não está mais em operação.

Dados comprometidos: cartões de crédito, endereços de e-mail, endereços IP, senhas, tíquetes de suporte, nomes de usuário

Ticketfly : Em maio de 2018, o site do serviço de distribuição de ingressos Ticketfly foi desfigurado por um invasor e posteriormente colocado offline . O invasor supostamente solicitou um resgate para compartilhar detalhes da vulnerabilidade com a Ticketfly, mas não recebeu uma resposta e posteriormente postou os dados violados online em um local acessível ao público. Os dados incluíam mais de 26 milhões de endereços de e-mail exclusivos, juntamente com nomes, endereços físicos e números de telefone. Embora não houvesse senhas nos dados vazados publicamente, a Ticketfly posteriormente emitiu uma atualização de incidente e afirmou que "é possível, no entanto, que valores com hash de credenciais de senha possam ter sido acessados".

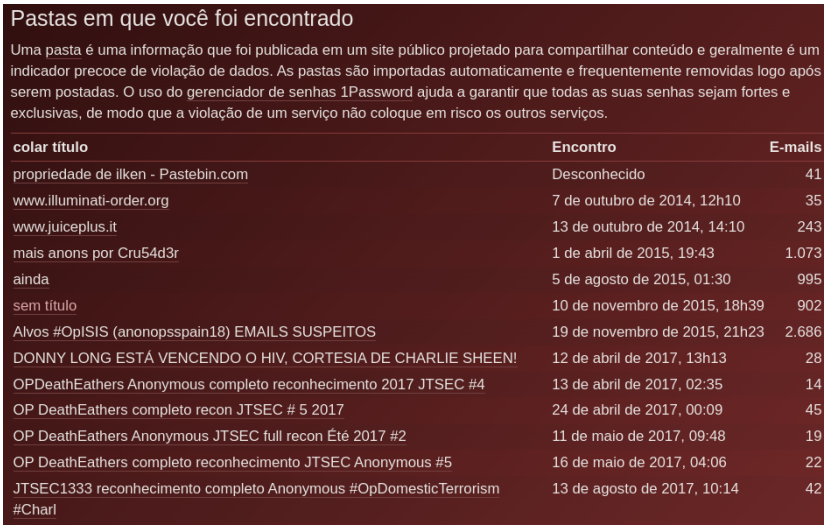
Dados comprometidos: endereços de e-mail, nomes, números de telefone, endereços físicos

WHMCS : Em maio de 2012, a empresa de hospedagem, cobrança e automação WHMCS sofreu uma violação de dados que expôs 134 mil endereços de e-mail. A violação incluiu informações extensas sobre clientes e históricos de pagamento, incluindo números parciais de cartão de crédito.

Dados comprometidos: endereços de e-mail, mensagens de e-mail, empregadores, endereços IP, nomes, dados parciais de cartão de crédito, senhas, históricos de pagamento, endereços físicos, atividade do site

ZAP-Hosting : em novembro de 2021, o host ZAP-Hosting sofreu uma violação de dados que expôs mais de 60 GB de dados contendo 746 mil endereços de e-mail exclusivos. A violação também continha logs de bate-papo de suporte, endereços IP, nomes, compras, endereços físicos e números de telefone.

Dados comprometidos: detalhes do agente do usuário do navegador, logs de bate-papo, endereços de e-mail, endereços IP, nomes, números de telefone, endereços físicos, compras



Pastas em que você foi encontrado

Uma pasta é uma informação que foi publicada em um site público projetado para compartilhar conteúdo e geralmente é um indicador precoce de violação de dados. As pastas são importadas automaticamente e frequentemente removidas logo após serem postadas. O uso do gerenciador de senhas 1Password ajuda a garantir que todas as suas senhas sejam fortes e exclusivas, de modo que a violação de um serviço não coloque em risco os outros serviços.

colar título	Encontro	E-mails
propriedade de ilken - Pastebin.com	Desconhecido	41
www.illuminati-order.org	7 de outubro de 2014, 12h10	35
www.juiceplus.it	13 de outubro de 2014, 14:10	243
mais anons por Cru54d3r	1 de abril de 2015, 19:43	1.073
ainda	5 de agosto de 2015, 01:30	995
sem título	10 de novembro de 2015, 18h39	902
Alvos #OpISIS (anonopsspain18) EMAILS SUSPEITOS	19 de novembro de 2015, 21h23	2.686
DONNY LONG ESTÁ VENCENDO O HIV, CORTESIA DE CHARLIE SHEEN!	12 de abril de 2017, 13h13	28
OPDeathEathers Anonymous completo reconhecimento 2017 JTSEC #4	13 de abril de 2017, 02:35	14
OP DeathEathers completo recon JTSEC # 5 2017	24 de abril de 2017, 00:09	45
OP DeathEathers Anonymous JTSEC full recon Été 2017 #2	11 de maio de 2017, 09:48	19
OP DeathEathers completo reconhecimento JTSEC Anonymous #5	16 de maio de 2017, 04:06	22
JTSEC1333 reconhecimento completo Anonymous #OpDomesticTerrorism #Charl	13 de agosto de 2017, 10:14	42

Recomendação	Atualizar os e-mails cadastrados e trocar senhas antigas por senhas novas e fortes o mais rápido possível.

10. QUADRO SWOT DA SEGURANÇA DO SITE

Forças: Certificado SSL emitido e API bem estruturada e configurada.
Fraquezas: Não identificadas.
Oportunidades: Diminuir possibilidades de engenharia social.
Ameaças: E-mails passíveis de serem invadidos e muitas portas abertas.

11. CONCLUSÕES E RECOMENDAÇÕES GERAIS

Conforme detalhado no item 6, e de acordo com as vulnerabilidades encontradas nos testes, é possível concluir que o sucesso de um ataque pode resultar em perdas financeiras, de ativos ou de recursos, além de causar danos à imagem da plataforma. Portanto, sua remediação é média para os negócios, exigindo que seja providenciada em curto intervalo de tempo. A abordagem dos testes realizados não considera a probabilidade do agente de ameaça, nem responde por qualquer um dos vários detalhes técnicos associados à sua aplicação específica. Qualquer um desses fatores poderia afetar significativamente a probabilidade global de um atacante encontrar e explorar uma vulnerabilidade particular. Esta classificação também não leva em conta o impacto real

sobre o negócio. É necessário que a área específica de segurança da plataforma defina qual o grau de risco de segurança das aplicações que está disposta a aceitar. Cabe ressaltar, que novas ameaças, novas vulnerabilidades e mudanças na probabilidade ou nas consequências podem vir a ampliar os riscos anteriormente avaliados como pequenos. Convém que a análise crítica dos riscos pequenos e aceitos considere cada risco separadamente e em conjunto, a fim de avaliar seu impacto potencial agregado. Se os riscos não estiverem dentro da categoria "informativo" ou "baixo", convém que eles sejam tratados utilizando-se uma ou mais de uma das opções consideradas.

12. REFERÊNCIAS

DNS Dumpster: **dns recon & research, find & lookup dns records**. 2019. EUA: Hacker Target Pty Ltd, 2007. Software de Pentest. Disponível em: https://dnsdumpster.com/. Acesso em: 27 nov. 2022.

BUILT With: **Find out what websites are Built With**. 2022. Level 35 One International Towers 100 Barangaroo Avenue Sydney NSW 2000 Australia: BuiltWith® Pty Ltd, 2007. Software de Pentest. Disponível em: https://builtwith.com/. Acesso em: 27 nov. 2022.

NMAP: **A Network Mapper**. 7.93. EUA: Gordon "Fyodor" Lyon, 1997. Software de Pentest. Acesso em: 27 nov. 2022.

SPIDERFOOT: **SpiderFoot automates OSINT so you can find what matters, faster**. 4.0. EUA: Steve Micallef, 2005. Software de Pentest. Disponível em: https://www.spiderfoot.net/. Acesso em: 27 nov. 2022.

HAVE I Been Pwned?: **Check if your email or phone is in a data breach**. 2022. EUA: TroyHunt, 2013. Software de Pentest. Disponível em: https://haveibeenpwned.com/. Acesso em: 27 nov. 2022.