

# OSINT FRAMEWORK & FOOTPRINTING

---

By Fareeha Naveed



## Table of Contents:

1. Disclaimer
2. Introduction to OSINT & Footprinting
3. Targeted Domain
4. Tasks & Findings
  - Task 1: Identify Domain Registrar, Creation Date, and Contacts (WHOIS Lookup)
  - Task 2: Checking the Data Breach of Abuse Email (Have I Been Pwned / Security Headers)
  - Task 3: Company and Technical Information (BuiltWith & Wappalyzer)
  - Task 4: Wayback Machine Analysis
  - Task 5: Enumerate Name Servers and IP Addresses (dig)

- Task 6: IP Address Information (ipinfo.io)
  - Task 7: Discover Subdomains (Sublist3r)
  - Task 8: Port Scanning and Service Detection (nmap)
  - Task 9: IP Address Searching (nslookup)
  - Task 10: Search for Public Email Addresses (theHarvester)
  - Task 11: Search Exposed Documents or Credentials (dnsenum)
  - Task 12: Check SSL/TLS Configuration (ssllscan)
  - Task 13: Check the Usernames (Sherlock)
  - Task 14: OSINT Visualization (SpiderFoot)
  - Task 15: Tracing the Route (traceroute)
  - Task 16: Google Dorking (Google)
  - Task 17: DNS and Subdomains detail (Dnsdumpster)
  - Task 18: Search Exposed Documents or Credentials (GitHub)
  - Task 19: Report Making (Shodan)
5. Case Study: Recent BMW Data Breach (2025)
  6. Conclusion
  7. References & Tools Used

## DISCLAIMER

This document has been created solely for educational and research purposes. The techniques, tools, and methods described for Open-Source Intelligence (OSINT) gathering and website footprinting are intended to enhance understanding of cybersecurity concepts.

The information on OSINT and website footprinting must not be used for unauthorized or malicious activities. Performing these techniques without proper consent may be illegal. The author assumes no responsibility for any misuse; users are solely responsible for ensuring legal and ethical use.

## INTRODUCTION to OSINT & FOOTPRINTING:

The **OSINT Framework** is a publicly available, web-based directory that organizes and categorizes hundreds of OSINT tools and resources, acting as a roadmap to help investigators find the right tools for their tasks.

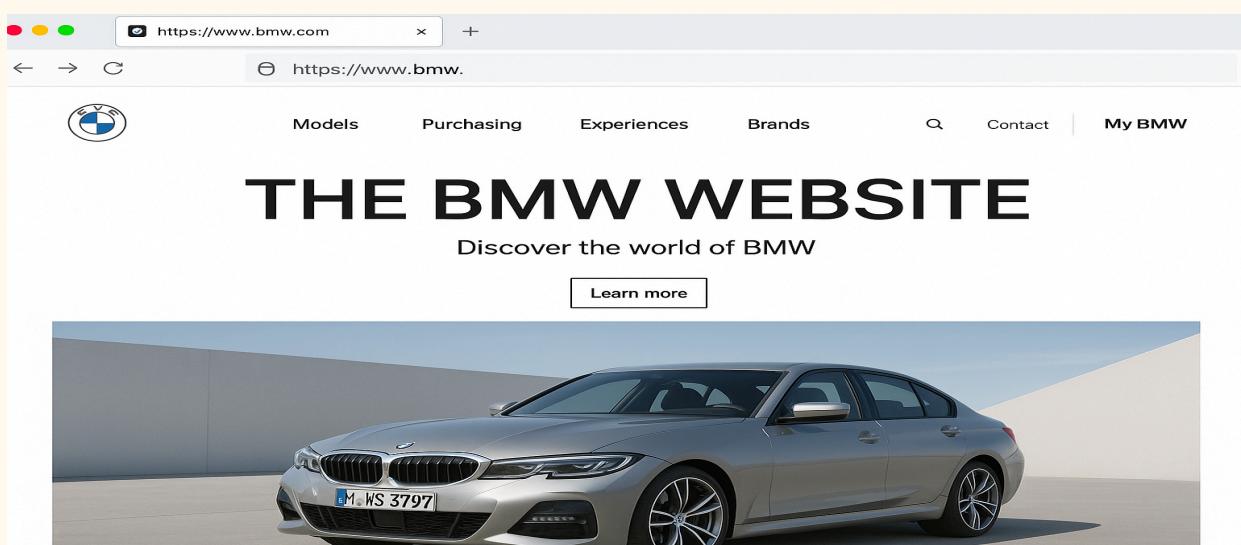
**Footprinting**, also known as reconnaissance, is a preliminary phase in penetration testing and ethical hacking, where an attacker gathers information about a target system or network before

launching an attack. This involves collecting data about the target's infrastructure, systems, and employees to identify potential vulnerabilities.

- Footprinting: is the initial phase of gathering information about a target.
- OSINT: is the method used to find this information by accessing public data.
- Together, they create a detailed picture of a target's digital footprint, revealing their online activities, connections, and vulnerabilities.

## TARGETED DOMAIN

The target website for this OSINT and footprinting exercise is [BMW.COM](https://www.bmw.com), the official online presence of Bayerische Motoren Werke AG (BMW Group), a globally recognized automobile manufacturer headquartered in Munich, Germany. In the context of footprinting, BMW.com will be analyzed to gather publicly available information about its infrastructure, technologies, and digital footprint. This process does not involve exploiting or attacking the system but focuses on collecting intelligence such as **domain details, DNS records, server information, hosting providers, SSL certificates, and other metadata** that help understand the site's architecture and exposure on the internet by using active and passive footprinting.



## TASK 1: Identify Domain Registrar, Creation Date, and Contacts

### APPROACH: Passive Reconnaissance

## TOOL USED: WHOIS LOOKUP / Whois [bmw.com](#) (in Kali)

The screenshot shows a Whois lookup result for the domain [bmw.com](#). The results are organized into three main sections: Domain Information, Registrar Information, and Registrant Contact.

**Domain Information:**

- Domain: [bmw.com](#)
- Registered On: 1996-01-29
- Expires On: 2033-01-30
- Updated On: 2024-01-30
- Status: server delete prohibited  
server transfer prohibited  
server update prohibited
- Name Servers: ns.bmw.de, ns2.m-online.net, ns3.m-online.net, ns4.m-online.net

**Registrar Information:**

- Registrar: CSC Corporate Domains, Inc.
- IANA ID: 299
- Abuse Email: [domainabuse@cscglobal.com](mailto:domainabuse@cscglobal.com)
- Abuse Phone: 8887802723

**Registrant Contact:**

- Organization: Bayerische Motoren Werke AG
- Country: DE
- Email: <https://domaincontact.cscglobal.com/contactholder/bmw.com/registrant>

## KEY FINDINGS:

### Domain Information

- Domain: [bmw.com](#)

- Registered On:1996-01-29
- Expires On:2033-01-30
- Updated On:2024-01-30

**Status:**

- server delete prohibited / server transfer prohibited / server update prohibited

**Name Servers:**

- ns.bmw.de
- ns2.m-online.net
- ns3.m-online.net
- ns4.m-online.net

**Registrar Information**

- Registrar: CSC Corporate Domains, Inc.
- IANA ID:299
- Abuse Email:domainabuse@cscglobal.com
- Abuse Phone:8887802723

**Registrant Contact**

- Organization: **Bayerische Motoren Werke AG**
- Country:DE
- Email: <https://domaincontact.cscglobal.com/contactholder/bmw.com/registrant>

**BMW is registered with CSC Corporate Domains on 29/01/1996 and is valid till 30/01/2033. It has HYBRID DNS CONFIGURATION SYSTEM. The name server [ns.bmw.de](#) is the custom domain of BMW and it is self hosted**

**We can use Kali Linux for these details or to cross check from both the sources. On terminal we found the Name Servers, Registrar IDs , Abuse emails and contact info , Domain of [bmw.com](#)**

```
(kali㉿kali)-[~]
$ whois bmw.com
Domain Name: BMW.COM
Registry Domain ID: 43804_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: http://cscdbs.com
Updated Date: 2024-01-30T14:18:40Z
Creation Date: 1996-01-29T05:00:00Z
Registry Expiry Date: 2033-01-30T05:00:00Z
Registrar: CSC Corporate Domains, Inc.
Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: 8887802723
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: NS.BMW.DE
Name Server: NS2.M-ONLINE.NET
Name Server: NS3.M-ONLINE.NET
Name Server: NS4.M-ONLINE.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-08-27T14:36:36Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.
```

## TASK 2 : CHECKING THE DATA BREACH OF ABUSE EMAIL

APPROACH: Passive Reconnaissance

TOOL USED: Have I been owned / Security Headers

The screenshot shows the Have I Been Pwned website interface. At the top, there is a search bar containing the email address "domainabuse@cscglobal.com" and a blue "Check" button. Below the search bar, a small note states "Using Have I Been Pwned is subject to the [terms of use](#)". The main section is titled "Email Breach History" and subtitle "Timeline of data breaches affecting your email address". A large red box highlights the number "7" followed by "Data Breaches". Below this, a message reads "Oh no — pwned! This email address has been found in multiple data breaches. Review the details below to see where your data was exposed." The background of the page is black.

**The abuse email which is registered in [bmw.com](#) has been breached over 7 times.**

The screenshot shows a security report summary for the domain "domainabuse@cscglobal.com". At the top, there is a search bar with the same email address and a "Scan" button. Below the search bar, there are two checkboxes: "Hide results" (unchecked) and "Follow redirects" (checked). The main section is titled "Security Report Summary". It includes a large orange square icon with a white letter "D". The report details the following information:

- Site:** <https://www.cscglobal.com/cscglobal/home/>
- IP Address:** 165.160.32.200
- Report Time:** 26 Aug 2025 10:02:52 UTC
- Headers:** A list of HTTP headers with status indicators:
  - ✓ X-Frame-Options
  - ✓ Strict-Transport-Security
  - ✗ Content-Security-Policy
  - ✗ X-Content-Type-Options
  - ✗ Referrer-Policy
  - ✗ Permissions-Policy
- Advanced:** A note stating "Your site could be at risk, let's perform a deeper security analysis of your site and APIs:" followed by a "Start Now" button.

**The IP address of abuse email is 165.160.32.200**

## TASK 3: COMPANY AND TECHNICAL INFORMATION

### APPROACH \_Passive Reconnaissance

### TOOLS USED Builtwith

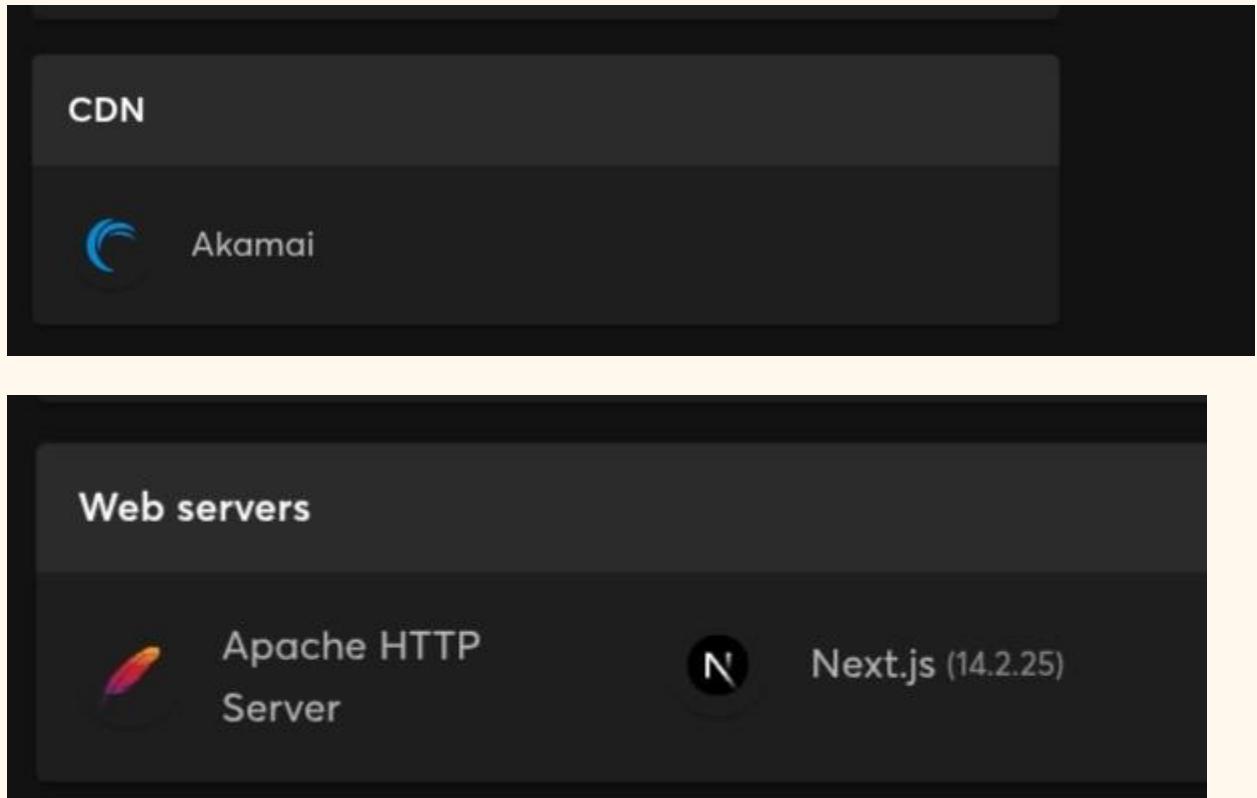
#### DETAILS : Company Information

- **Company Name:** Bayerische Motoren Werke AG
- **Location:** Munich, 80788, Germany
- **Vertical:** Automotive and Vehicles
- **Estimated Employees:** 100,000+ (This is a global figure for the entire company, not just the web team).
  - Referring IPs: 10,377 (IP addresses that link to bmw.com).
  - URLs: 6,728 (An estimate of the number of pages on the site).
  - Subnets: 100,000+ (A large number of associated network blocks, indicating a massive online infrastructure).

The screenshot shows a search result for "BMW.COM" on the Builtwith platform. The main heading is "BMW.COM". Below it is a navigation bar with tabs: Technology Profile, Detailed, Meta (which is highlighted), Products, People, Redirect, AI, Recommendations, and Company. The "Meta" section contains contact information for the company.

Contact Information		
Company Name	Bayerische Motoren Werke AG <a href="#">Find People on LinkedIn</a>	
Location	Munich 80788 Germany	Telephone

### RESULTS BY USING WAPALYZER



## RESULTS BY USING BUILT WITH

SSL Certificates			
 SSL by Default		Aug 2023	Aug 2025
 SwissSign		Apr 2023	Aug 2025
 GlobalSign	Root Authority	May 2017	Aug 2025
Web Servers			
 Apache		Dec 2011	Aug 2025
Operating Systems and Servers			
 IPv6		Oct 2024	Aug 2025
Verified CDN			
 Akamai Edge	Edge Delivery Network	Oct 2014	Aug 2025 

JavaScript libraries

	core-js (3.40.0)		Boomerang
	Swiper		jQuery UI (1.13.3)
	lit-element (4.1.1)		Lodash (4.17.21)
	lit-html (3.2.1)		jQuery (3.6.0)
	Apollo		

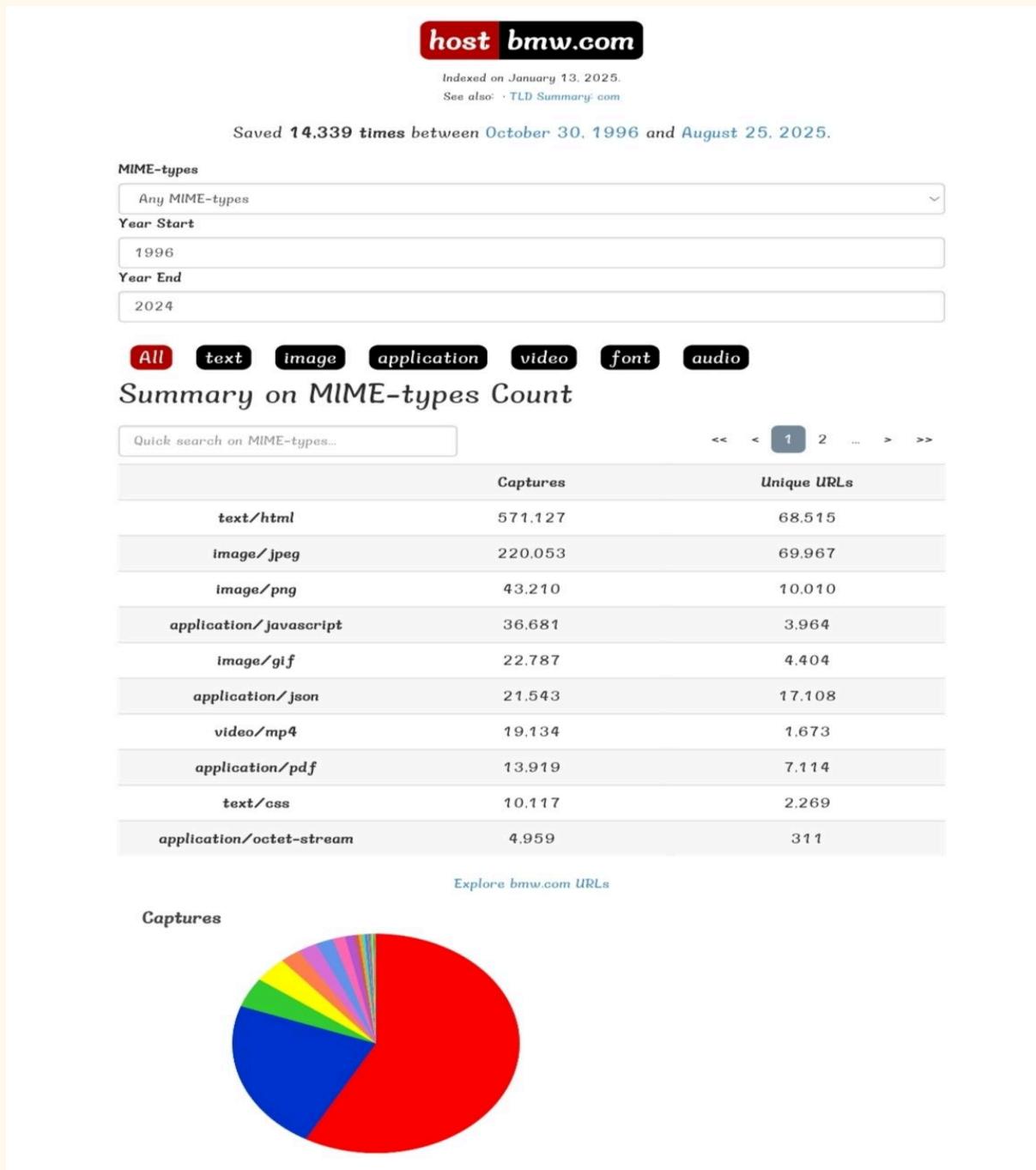
Category	Technology	Source
Web Server	Apache	Builtwith & Wapalyzer
Operating System	IPv6	Builtwith
SSL Certificate	SSL by default	Builtwith
JavaScript Libraries	jQuery UI · jQuery, Apollo	Wapalyzer & Builtwith
CDN	Akamai	Builtwith & Wapalyzer

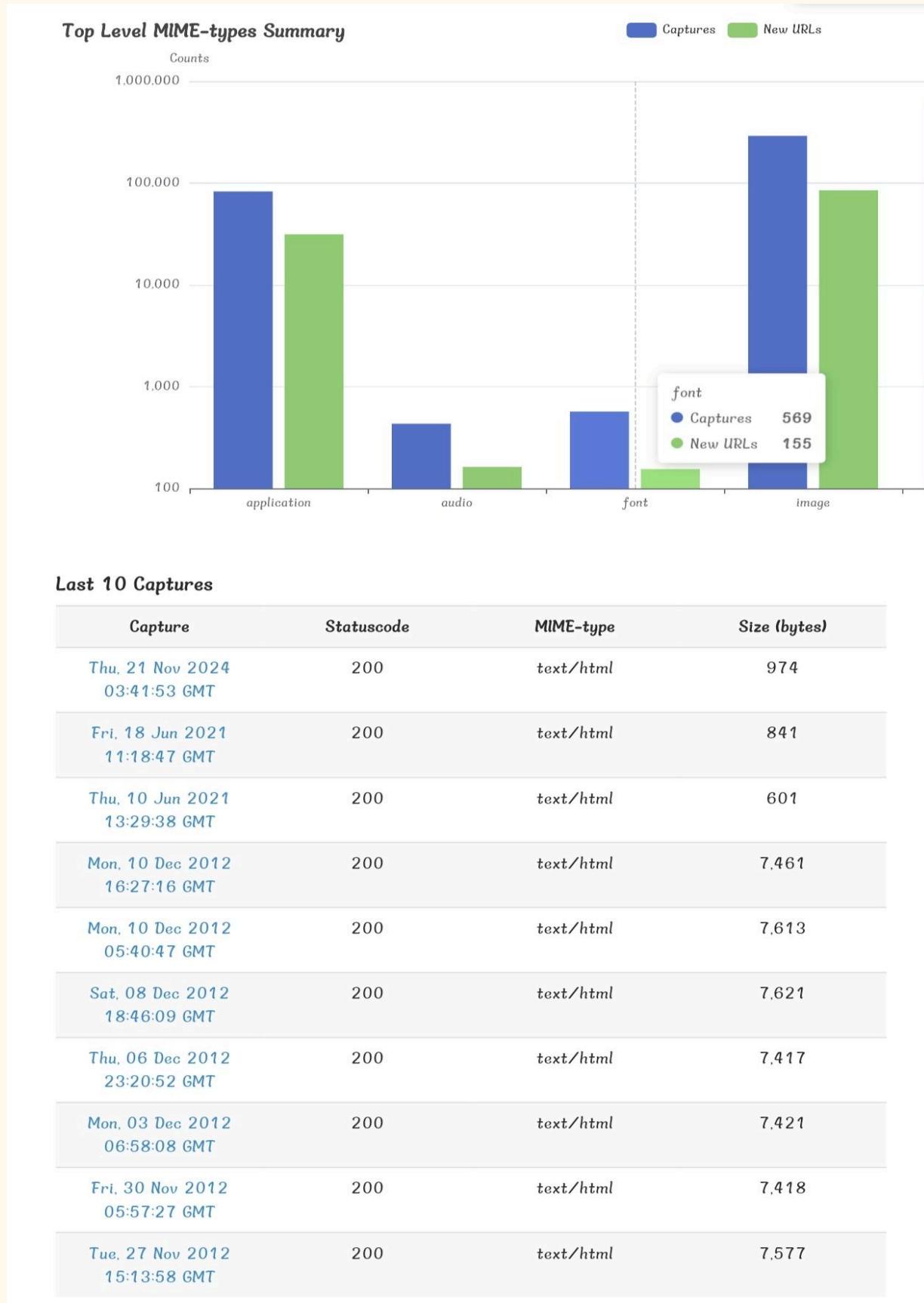
Through passive reconnaissance using Wappalyzer and BuiltWith, several key technologies in use by BMW com were identified. The website previously used the Apache web server, while current technologies include SSL, and the jQuery 1.8.1 JavaScript library. Akamai Edge is used for CDN and DNS services. These findings suggest a mix of legacy and modern technologies with a focus on open-source tools and basic security implementation

## TASK 4 : WAY BACK MACHINE ANALYSIS

### APPROACH Passive Reconnaissance

### TOOL USED Wayback Machine





## Key Overview:

- First Capture: October 30, 1996
- Last Capture: November 21, 2024 (as of this data)
- Total Captures: 14,339 times
- Indexing Date: This data was compiled on January 13, 2025.

**There was a significant and sustained period of frequent archiving between approximately 2004 and 2016. Before 2004, captures were less frequent (as the web and the Archive were younger). After 2016, the frequency of captures appears to have decreased noticeably.**

## TASK 5: Enumerate Name servers and IP Addresses

### APPROACH: Passive Reconnaissance

### TOOL USED: dig

```
(kali㉿kali)-[~]
$ dig bmw.com

; <>> DIG 9.20.9-1-Debian <>> bmw.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55042
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;;
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 1232
;; COOKIE: a235a5c26401d05c0100000068ad87f2abe504c4e150b8d8 (good)
;; QUESTION SECTION:
;bmw.com.           IN      A

;; ANSWER SECTION:
bmw.com.          5       IN      A      160.46.226.165

;; Query time: 223 msec
;; SERVER: 192.168.136.2#53(192.168.136.2) (UDP)
;; WHEN: Tue Aug 26 06:09:54 EDT 2025
;; MSG SIZE  rcvd: 80
```

- IP Address **160.46.226.165**
- DNS SERVER **192.168.136.2**

The tool (dig) directly sent a UDP DNS query packet to a DNS server (192.168.136.2) asking for the bmw.com record.

## TASK 6: IP ADDRESS INFORMATION

### APPROACH: Passive Reconnaissance

#### TOOL USED: [ipinfo.io](https://ipinfo.io/)

```
{
  "ip": "160.46.226.165",
  "asn": "AS8590",
  "as_name": "Bayerische Motoren Werke Aktiengesellschaft",
  "as_domain": "bmw.com",
  "country_code": "DE",
  "country": "Germany",
  "continent_code": "EU",
  "continent": "Europe"
}
```

#### 1. Network Ownership (ASN):

- Autonomous System Number: AS8590 (Note: The first image had a typo, AS5599; the correct ASN is AS8590).
- Registered Owner: Bayerische Motoren Werke Aktiengesellschaft (BMW AG)

- ASN Type: Hosting. This indicates the network is used to host BMW's internet services (websites, APIs, etc.), not just for corporate office connectivity.
- Network Range: 160.46.224.0/19
- This is a large block containing 8,190 IP addresses, all belonging to BMW.

## 2. Geolocation:

- City: Freising, Bavaria
- Country: Germany (DE)
- Coordinates: 48.4035, 11.7488
- This suggests the physical location of the data center or network egress point for this IP address.

## TASK 7: DISCOVER SUBDOMAINS

**APPROACH:** Passive Reconnaissance

**TOOL USED:** Sublist3r

The core function of Sublist3r is to discover as many subdomains associated with a domain as possible. For example, for example.com, it would try to find subdomains

- By using the sublist3r tool I have discovered the subdomains of the main domain used in [BMW.COM](#)

```
(kali㉿kali)-[~]
$ sublist3r -d bmw.com

Sublist3r
# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for bmw.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
Process DNSdumpster-8:
Traceback (most recent call last):
  File "/usr/lib/python3.13/multiprocessing/process.py", line 313, in _bootstrap
    self.run()
      ^^^^^^
  File "/usr/lib/python3/dist-packages/sublist3r.py", line 269, in run
    domain_list = self.enumerate()
  File "/usr/lib/python3/dist-packages/sublist3r.py", line 649, in enumerate
    token = self.get_csrftoken(resp)
  File "/usr/lib/python3/dist-packages/sublist3r.py", line 644, in get_csrftoken
    token = csrf_regex.findall(resp)[0]
          ^^^
IndexError: list index out of range

[-] Total Unique Subdomains Found: 12
www.bmw.com
auth.bmw.com
b2b.bmw.com
b2bua.bmw.com
baonline.bmw.com
developer.bmw.com
exd-prod.bmw.com
lifestyle.bmw.com
nspeuwebp.bmw.com
pita-b2b.bmw.com
static.bmw.com
xpita-b2b.bmw.com
```

**The enumeration discovered 12 unique subdomains, revealing several key aspects of BMW's online infrastructure**

### TASK 8: Port Scanning and Service Detection

#### APPROACH Passive Reconnaissance

## TOOLS USED nmap

```
(kali㉿kali)-[~]
$ nmap -sV bmw.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-26 06:17 EDT
Nmap scan report for bmw.com (160.46.226.165)
Host is up (0.014s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd
443/tcp   open  ssl/http Apache httpd

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 92.86 seconds
```

Nmap identified two open ports on [BMW.COM](https://bmw.com) : port 80 (HTTP) and port 443 (HTTPS), both running HAProxy, a popular high-performance load balancer. This setup confirms the use of a reverse proxy or load balancer to manage incoming traffic.

## TASK 9: IP ADDRESS SEARCHING

### APPROACH: Passive Reconnaissance

### TOOL USED: nslookup

```
(kali㉿kali)-[~]
$ nslookup bmw.com
Server:          192.168.136.2
Address:         192.168.136.2#53

Non-authoritative answer:
Name:   bmw.com
Address: 160.46.226.165
```

- Thus the IP address of server is 192.168.136.2 and it sent packets via port 53
- The IP address of the site [bmw.com](https://bmw.com) is 160.46.226.165

## TASK 10: SEARCH FOR PUBLIC EMAIL ADDRESSES

## APPROACH: Passive Reconnaissance

### TOOL USED theHarvester



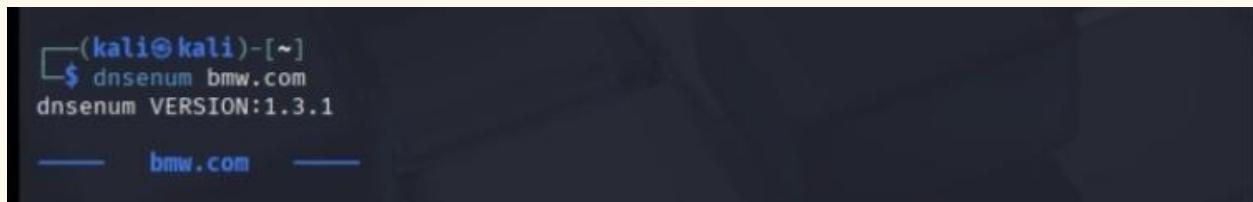
```
(kali㉿kali)-[~]
$ theHarvester -d bmw.com -b google -b bing -b yahoo
Read proxies.yaml from /etc/theHarvester/proxies.yaml
*****
* [REDACTED] FIREWALL [REDACTED] *
*****
* theHarvester 4.8.0
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*
*****
[*) Target: bmw.com
[*) Searching Yahoo.
[*) No IPs found.
[*) No emails found.
[*) No people found.
[*) Hosts found: 0
```

theHarvester revealed no public email addresses linked to bmw.com. It has identified no subdomains.

### TASK 11: SEARCH EXPOSED DOCUMENTS OR CREDENTIALS

#### APPROACH: Active Reconnaissance

#### TOOL USED: dnsenum



```
(kali㉿kali)-[~]
$ dnsenum bmw.com
dnsenum VERSION:1.3.1
— bmw.com —
```

Host's addresses:				
bmw.com.	5	IN	A	160.46.226.165
Name Servers:				
ns.bmw.de.	5	IN	A	192.109.190.2
ns2.m-online.net.	5	IN	A	212.18.3.8
ns3.m-online.net.	5	IN	A	217.160.41.67
ns4.m-online.net.	5	IN	A	212.114.171.64

**Its primary purpose is to perform comprehensive DNS enumeration of a target domain. It is significantly more aggressive and detailed than a simple dig or nslookup command**

#### 1. ns.bmw.de

- IP: 192.109.190.2
- Significance: This is a name server under BMW's own .de domain, suggesting they manage part of their DNS infrastructure internally.

#### 2. ns2.m-online.net

- IP: 212.18.3.8

#### 3. ns3.m-online.net

- IP: 217.160.41.67

#### 4. ns4.m-online.net

- IP: 212.114.171.64

**MAIL MX SERVER :** An MX mail server is the actual email server that receives email for a specific domain, as designated by an MX record (Mail eXchanger record) in the Domain Name System (DNS).

<b>Mail (MX) Servers:</b>				
mx1.hc324-48.eu.iphmx.com.	5	IN	A	207.54.72.35
mx1.hc324-48.eu.iphmx.com.	5	IN	A	207.54.69.24
mx1.hc324-48.eu.iphmx.com.	5	IN	A	207.54.69.27
mx1.hc324-48.eu.iphmx.com.	5	IN	A	207.54.71.69
mx1.hc324-48.eu.iphmx.com.	5	IN	A	207.54.65.242
mx1.hc324-48.eu.iphmx.com.	5	IN	A	207.54.68.120
mx1.hc324-48.eu.iphmx.com.	5	IN	A	207.54.71.60
mx1.hc324-48.eu.iphmx.com.	5	IN	A	207.54.68.119
mx1.hc324-48.eu.iphmx.com.	5	IN	A	207.54.71.126
mx1.hc324-48.eu.iphmx.com.	5	IN	A	207.54.69.30
mx1.hc324-48.eu.iphmx.com.	5	IN	A	207.54.69.29
mx1.hc324-48.eu.iphmx.com.	5	IN	A	207.54.71.48
mx1.hc324-48.eu.iphmx.com.	5	IN	A	207.54.68.121
mx1.hc324-48.eu.iphmx.com.	5	IN	A	207.54.72.34
mx2.hc324-48.eu.iphmx.com.	5	IN	A	207.54.72.34
mx2.hc324-48.eu.iphmx.com.	5	IN	A	207.54.71.48
mx2.hc324-48.eu.iphmx.com.	5	IN	A	207.54.68.119
mx2.hc324-48.eu.iphmx.com.	5	IN	A	207.54.65.242
mx2.hc324-48.eu.iphmx.com.	5	IN	A	207.54.71.69
mx2.hc324-48.eu.iphmx.com.	5	IN	A	207.54.69.27
mx2.hc324-48.eu.iphmx.com.	5	IN	A	207.54.68.121
mx2.hc324-48.eu.iphmx.com.	5	IN	A	207.54.69.29
mx2.hc324-48.eu.iphmx.com.	5	IN	A	207.54.68.120
mx2.hc324-48.eu.iphmx.com.	5	IN	A	207.54.69.24
mx2.hc324-48.eu.iphmx.com.	5	IN	A	207.54.69.30
mx2.hc324-48.eu.iphmx.com.	5	IN	A	207.54.71.126
mx2.hc324-48.eu.iphmx.com.	5	IN	A	207.54.71.60
mx2.hc324-48.eu.iphmx.com.	5	IN	A	207.54.72.35

**Multiple IP addresses are mapped for redundancy, load balancing, and resilience. If one server is down, others can still handle mail delivery.**

### **Resolved IP Addresses:**

**The MX records resolve to multiple IP addresses, such as:**

**207.54.72.35**

**207.54.65.242**

**207.54.69.24**

**207.54.68.120**

**207.54.69.27**

**207.54.71.60**

**207.54.71.69**

**207.54.68.119**

207.54.71.126	207.54.71.48
207.54.69.30	207.54.68.1
207.54.69.29	

### ZONE TRANSFER ATTEMPTS

```
Trying Zone Transfers and getting Bind Versions:  
  
Trying Zone Transfer for bmw.com on ns2.m-online.net ...  
AXFR record query failed: REFUSED  
  
Trying Zone Transfer for bmw.com on ns4.m-online.net ...  
AXFR record query failed: REFUSED  
  
Trying Zone Transfer for bmw.com on ns3.m-online.net ...  
AXFR record query failed: REFUSED  
  
Trying Zone Transfer for bmw.com on ns.bmw.de ...  
AXFR record query failed: REFUSED
```

**All the DNS servers were refused This demonstrates that zone transfers are securely configured and restricted, preventing unauthorized access to the entire DNS zone data.**

### BRUTE FORCE SUBDOMAINS

**Brute force is a cybersecurity attack method where an attacker uses automated tools to systematically try every possible combination of passwords, usernames, or encryption keys until they successfully gain unauthorized access to a system or account.**

<b>Brute Forcing with /usr/share/dnsenum/dns.txt:</b>					
asc.bmw.com.	5	IN	A	160.46.235.194	
beta.bmw.com.	5	IN	CNAME	bmwprod.b.edgekey.net.	
bmwprod.b.edgekey.net.	5	IN	CNAME	e25631.dsca.akamaiedge.net.	
e25631.dsca.akamaiedge.net.	5	IN	A	23.215.7.19	
e25631.dsca.akamaiedge.net.	5	IN	A	23.215.7.4	
fr.bmw.com.	5	IN	A	160.46.247.181	
ftp.bmw.com.	5	IN	A	195.27.218.60	
nic.bmw.com.	5	IN	A	185.16.184.143	
rcc.bmw.com.	5	IN	CNAME	ocapi.aws.bmw.cloud.	
ocapi.aws.bmw.cloud.	5	IN	A	18.64.141.44	
ocapi.aws.bmw.cloud.	5	IN	A	18.64.141.102	
ocapi.aws.bmw.cloud.	5	IN	A	18.64.141.38	
ocapi.aws.bmw.cloud.	5	IN	A	18.64.141.101	
search.bmw.com.	5	IN	A	62.67.62.32	
shop.bmw.com.	5	IN	CNAME	wcmp.edgekey.net.	
wcmp.edgekey.net.	5	IN	CNAME	e25631.dsca.akamaiedge.net.	
e25631.dsca.akamaiedge.net.	5	IN	A	2.16.158.234	
e25631.dsca.akamaiedge.net.	5	IN	A	104.116.245.89	
static.bmw.com.	5	IN	CNAME	bmwprod.edgekey.net.	
bmwprod.edgekey.net.	5	IN	CNAME	e12267.dsca.akamaiedge.net.	
e12267.dsca.akamaiedge.net.	5	IN	A	104.116.245.83	
e12267.dsca.akamaiedge.net.	5	IN	A	104.116.245.120	
vpn.bmw.com.	5	IN	A	193.23.39.10	
vpn2.bmw.com.	5	IN	A	193.23.33.6	
www.bmw.com.	5	IN	CNAME	bmwprod.b-ion.edgekey.net.	
bmwprod.b-ion.edgekey.net.	5	IN	CNAME	e25631.dsca.akamaiedge.net.	
e25631.dsca.akamaiedge.net.	5	IN	A	23.215.7.19	
e25631.dsca.akamaiedge.net.	5	IN	A	23.215.7.4	
www2.bmw.com.	5	IN	CNAME	www2.bmw.com.c.footprint.net.	

**The brute-force attack successfully discovered 13 subdomains, revealing a multi-layered and well-protected infrastructure.**

### CLASS ‘C’ NETRANGES

<b>bmw.com class C netranges:</b>	
62.67.62.0/24	
160.46.226.0/24	
160.46.235.0/24	
160.46.247.0/24	
185.16.184.0/24	
193.23.33.0/24	
193.23.39.0/24	
195.27.218.0/24	

**The DNS enumeration for bmw.com revealed multiple class C netblocks (e.g., 62.67.62.0/24, 160.46.226.0/24, 193.23.33.0/24) associated with BMW's infrastructure. These IP ranges host various subdomains and services**

### TASK 12: CHECK SSL / TSL CONFIGURATION

#### APPROACH Active Reconnaissance

#### TOOL USED ssllscan

```
(kali㉿kali)-[~]
$ ssllscan bmw.com
Version: 2.1.5
OpenSSL 3.5.0 8 Apr 2025

Connected to 160.46.226.165

Testing SSL server bmw.com on port 443 using SNI name bmw.com

SSL/TLS Protocols:
SSLv2      disabled
SSLv3      disabled
TLSv1.0    disabled
TLSv1.1    disabled
TLSv1.2    enabled
TLSv1.3    enabled

TLS Fallback SCSV:
Server supports TLS Fallback SCSV

TLS renegotiation:
Session renegotiation not supported

TLS Compression:
Compression disabled

Heartbleed:
TLSv1.3 not vulnerable to heartbleed
TLSv1.2 not vulnerable to heartbleed

Supported Server Cipher(s):
Preferred TLSv1.3 256 bits TLS_AES_256_GCM_SHA384      Curve 25519 DHE 253
Accepted   TLSv1.3 256 bits TLS_CHACHA20_POLY1305_SHA256 Curve 25519 DHE 253
Accepted   TLSv1.3 128 bits TLS_AES_128_GCM_SHA256       Curve 25519 DHE 253
Preferred TLSv1.2 256 bits ECDHE-RSA-AES256-GCM-SHA384  Curve 25519 DHE 253
Accepted   TLSv1.2 256 bits ECDHE-RSA-CHACHA20-POLY1305 Curve 25519 DHE 253
Accepted   TLSv1.2 128 bits ECDHE-RSA-AES128-GCM-SHA256  Curve 25519 DHE 253
```

Property	Details
Server IP	160.46.226.165
TLS Supporting Version	TLS v1.2
Disabled Protocols	SSL v2, SSL v2 , TLS v1.0 , TLS v1.1 , TLS v1.3

## SERVER KEY EXCHANGE GROUP:

The Server Key Exchange message is a step in the TLS handshake where the server sends its cryptographic key to the client. This is necessary for certain key exchange algorithms where the server's certificate alone is not sufficient to establish a shared secret.

```
Server Key Exchange Group(s):
TLSv1.3 128 bits secp256r1 (NIST P-256)
TLSv1.3 192 bits secp384r1 (NIST P-384)
TLSv1.3 260 bits secp521r1 (NIST P-521)
TLSv1.3 128 bits x25519
TLSv1.3 224 bits x448
TLSv1.2 128 bits secp256r1 (NIST P-256)
TLSv1.2 192 bits secp384r1 (NIST P-384)
TLSv1.2 260 bits secp521r1 (NIST P-521)
TLSv1.2 128 bits x25519
TLSv1.2 224 bits x448
```

The server's TLS configuration supports a robust and modern set of key exchange groups across both TLSv1.2 and TLSv1.3 protocols. This indicates a strong emphasis on security and compatibility.

## SSL CERTIFICATE:

An SSL (Secure Sockets Layer) certificate, now more accurately called a TLS (Transport Layer Security) certificate, is a digital document that binds a cryptographic key to the details of an organization, server, or entity.

```

SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength: 2048

Subject: www-origin-proda2.bmw.com
AltNames: DNS:www-origin-proda2.bmw.com, DNS:bmwmyanmar.com, DNS:bmwlat.com, DNS:bmwbkk.de, DNS:bmw.vn, DNS:bmw.ua, DNS:bmw.tt, DNS:bmw.tm, DNS:bmw.sr, DNS:bmw.bn, DNS:bmw.sk, DNS:bmw.si, DNS:bmw.se, DNS:bmw.rs, DNS:bmw.ro, DNS:bmw.re, DNS:bmw.pt, DNS:bmw.pl, DNS:bmw.no, DNS:bmw.nl, DNS:bmw.mu, DNS:bmw.mq, DNS:bmw.mm, DNS:bmw.md, DNS:bmw.ma, DNS:bmw.ly, DNS:bmw.lv, DNS:bmw.lk, DNS:bmw.lc, DNS:bmw.kg, DNS:bmw.it, DNS:bmw.is, DNS:bmw.in, DNS:bmw.ie, DNS:bmw.ht, DNS:bmw.hn, DNS:bmw.gr, DNS:bmw.jp, DNS:bmw.fr, DNS:bmw.fi, DNS:bmw.es, DNS:bmw.dz, DNS:bmw.dk, DNS:bmw.de, DNS:bmw.cz, DNS:bmw.com.ve, DNS:bmw.com.uv, DNS:bmw.com.tr, DNS:bmw.com.sv, DNS:bmw.com.sg, DNS:bmw.com.py, DNS:bmw.com.ph, DNS:bmw.com.pe, DNS:bmw.com.pa, DNS:bmw.com.ni, DNS:bmw.com.my, DNS:bmw.com.mx, DNS:bmw.com.mt, DNS:bmw.com.mk, DNS:bmw.com.ky, DNS:bmw.com.kh, DNS:bmw.com.gt, DNS:bmw.com.ec, DNS:bmw.com.do, DNS:bmw.com.co, DNS:bmw.com.br, DNS:bmw.com.bo, DNS:bmw.com.bn, DNS:bmw.com.ar, DNS:bmw.com, DNS:bmw.co.za, DNS:bmw.co.uk, DNS:bmw.co.nz, DNS:bmw.co.jp, DNS:bmw.co.il, DNS:bmw.co.id, DNS:bmw.co.cr, DNS:bmw.co.ao, DNS:bmw.cl, DNS:bmw.ch, DNS:bmw.cc, DNS:bmw.ca, DNS:bmw.by, DNS:bmw.bs, DNS:bmw.bn, DNS:bmw.bg, DNS:bmw.bb, DNS:bmw.at, DNS:bmw-voli.me, DNS:bmw-tu-nisia.com, DNS:bmw-special-sales.com, DNS:bmw-nigeria.com, DNS:bmw-motorsport.com, DNS:bmw-me.com, DNS:bmw-m.com, DNS:bmw-golfsport.com, DNS:bmw-egypt.com
Issuer: GlobalSign RSA OV SSL CA 2018

Not valid before: May 8 08:26:12 2025 GMT
Not valid after: Jun 9 08:26:11 2026 GMT

```

Field	Value
Signature Algorithm	sha256WithRSAEncryption
RSA Key Strength	2048
Subject (Main Name)	ww-origin-proda2.bmw.com
Alt. Names	1. <a href="#">wa-origin-proda2.bmw.com</a> 2. <a href="#">bmw.sn</a> . 3. <a href="#">bmw.sk</a> 4. <a href="#">bmw.si</a> and many more....
Issuer Name	GlobalSign RSA OV SSL CA 2018
Valid From	May 8 08:26:12 2025 GMT
Valid till	Jun 9 08:26:11 2026 GMT

- The issuer indicates this is an Organization Validated (OV) SSL certificate, meaning GlobalSign verified BMW's organizational identity before issuance
- Key Strength: RSA 2048-bit. This is a currently accepted standard, though the industry is moving towards ECC keys for better performance and security.

## TASK 13: CHECK THE USERNAMES

### APPROACH: Passive Reconnaissance

## TOOLS USED: sherlock

```
(kali㉿kali)-[~]
└─$ sherlock bmw.com
[*] Checking username bmw.com on:

[+] BugCrowd: https://bugcrowd.com/bmw.com
[+] Cults3D: https://cults3d.com/en/users/bmw.com/creations
[+] Discord: https://discord.com
[+] Duolingo: https://www.duolingo.com/profile/bmw.com
[+] EyeEm: https://www.eyeem.com/u/bmw.com
[+] GNOME VCS: https://gitlab.gnome.org/bmw.com
[+] Giphy: https://giphy.com/bmw.com
[+] HackerEarth: https://hackerearth.com/@bmw.com
[+] HackerOne: https://hackerone.com/bmw.com
[+] kaskus: https://www.kaskus.co.id/@bmw.com
[+] Mydramalist: https://www.mydramalist.com/profile/bmw.com
[+] NationStates Nation: https://nationstates.net/nation=bmw.com
[+] NationStates Region: https://nationstates.net/region=bmw.com
[+] PCGamer: https://forums.pcgamer.com/members/?username=bmw.com
[+] PepperIT: https://www.pepper.it/profile/bmw.com/overview
[+] Snapchat: https://www.snapchat.com/add/bmw.com
[+] Spotify: https://open.spotify.com/user/bmw.com
[+] Tellonym.me: https://tellonym.me/bmw.com
[+] Weblate: https://hosted.weblate.org/user/bmw.com/
[+] YandexMusic: https://music.yandex/users/bmw.com/playlists
[+] omg.lol: https://bmw.com.omg.lol
[+] svidbook: https://www.svidbook.ru/user/bmw.com
[+] threads: https://www.threads.net/@bmw.com

[*] Search completed with 23 results
```

The Sherlock tool searched for the username bmw.com across numerous social media and online platforms. The scan returned 23 results, indicating that this username is registered on a variety of sites.

- BugCrowd: <https://bugcrowd.com/bmw.com>.
- Cults3D: <https://cults3d.com/en/users/bmw.com/creations>.
- Discord: <https://discord.com>.
- Duolingo: <https://www.duolingo.com/profile/bmw.com>.
- EyeEm: <https://www.eyeem.com/u/bmw.com>.

- Giphy: <https://giphy.com/bmw.com>.
- HackerEarth: <https://hackerearth.com/@bmw.com>.
- HackerOne: <https://hackerone.com/bmw.com>.
- kaskus: <https://www.kaskus.co.id/@bmw.com>.
- LibraryThing: <https://www.librarything.com/profile/bmw.com>.
- Mydramalist: <https://www.mydramalist.com/profile/bmw.com>.
- NationStates Nation: <https://nationstates.net/nation=bmw.com>.
- NationStates Region: <https://nationstates.net/region=bmw.com>.
- PCGamer:  
<https://forums.pcgamer.com/members/?username=bmw.com>.
- PepperIT: <https://www.pepper.it/profile/bmw.com/overview>.
- Snapchat: <https://www.snapchat.com/add/bmw.com>.
- Spotify: <https://open.spotify.com/user/bmw.com>.
- Tellonym.me: <https://tellonym.me/bmw.com>.
- Weblate: <https://hosted.weblate.org/user/bmw.com/>.
- YandexMusic: <https://music.yandex/users/bmw.com/playlists>.
- omg.lol: <https://bmw.com.omg.lol>
- threads: <https://www.threads.net/@bmw.com>

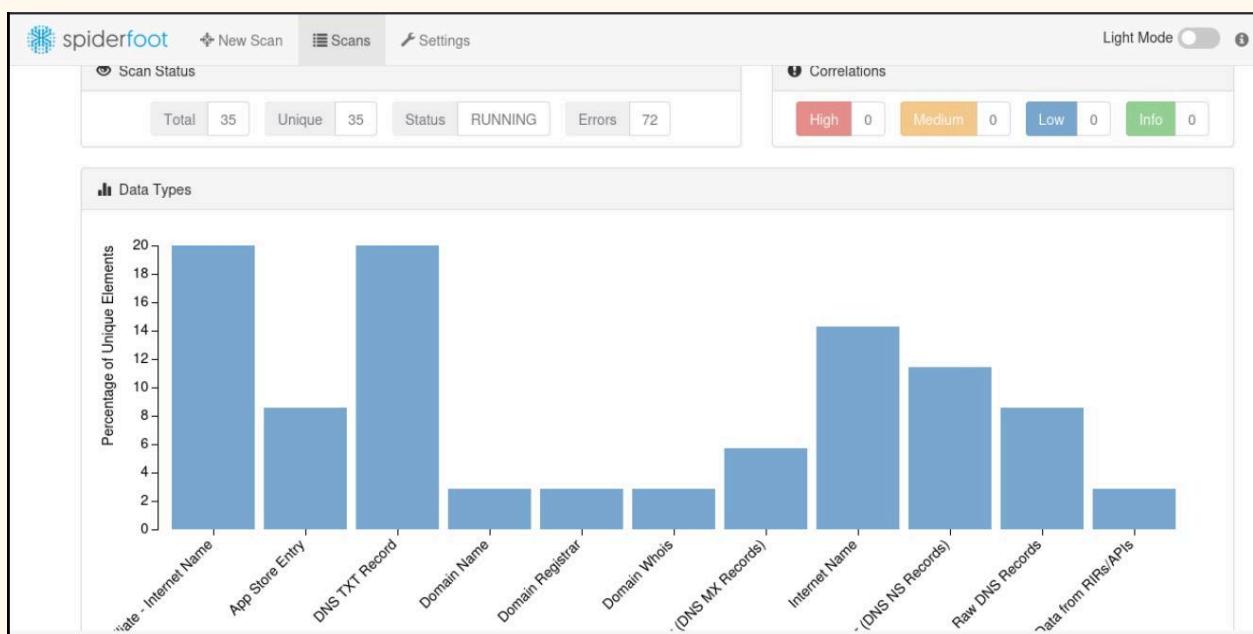
## **TASK 14: OSINT VISUALISATION**

**APPROACH:** Passive Reconnaissance

**TOOLS USED:** spiderfoot

```
(kali㉿kali)-[~]
$ spiderfoot -l 127.0.0.1:5001

*****
Use SpiderFoot by starting your web browser of choice and
browse to http://127.0.0.1:5001/
*****
2025-08-26 14:29:45,235 [INFO] sf : Starting web server at 127.0.0.1:5001 ... Log
2025-08-26 14:29:45,247 [WARNING] sf :
*****
Warning: passwd file contains no passwords. Authentication disabled.
Please consider adding authentication to protect this instance!
Refer to https://www.spiderfoot.net/documentation/#security.
*****
```



The screenshot shows the SpiderFoot web interface. At the top, there are navigation links: New Scan, Scans, Settings, Light Mode, and About. The main title is "Spider\_foot RUNNING". Below the title is a toolbar with icons for Summary, Correlations, Browse, Graph, Scan Settings, Log, and a search bar. The main content area is a table showing data types and their statistics:

Type	Unique Data Elements	Total Data Elements	Last Data Element
Affiliate - Internet Name	7	7	2025-08-26 14:56:03
App Store Entry	3	3	2025-08-26 14:55:13
DNS TXT Record	7	7	2025-08-26 14:56:03
Domain Name	1	1	2025-08-26 14:55:03
Domain Registrar	1	1	2025-08-26 14:55:06
Domain Whois	1	1	2025-08-26 14:55:06
Email Gateway (DNS MX Records)	2	2	2025-08-26 14:56:02
Internet Name	5	5	2025-08-26 14:56:47
Name Server (DNS NS Records)	4	4	2025-08-26 14:56:03
Raw DNS Records	3	3	2025-08-26 14:56:03
Raw Data from RIRs/APIs	1	1	2025-08-26 14:55:13

- Sensitive Info Found:** Multiple hacked email addresses and malicious/blacklisted domains related to [bmw.com](#).
- OSINT Scope:** The domain is linked to various usernames, SSL certs, and exposed repositories.
- Security Gaps:** Unresolved hostnames and publicly available internal links may indicate recon entry points.

## TASK 15: TRACING THE ROUTE

**APPROACH:** Passive Reconnaissance

**TOOLS USED:** traceroute

```
(kali㉿kali)-[~]
└─$ traceroute 160.46.226.165
traceroute to 160.46.226.165 (160.46.226.165), 30 hops max, 60 byte packets
 1  192.168.136.2 (192.168.136.2)  0.432 ms  0.296 ms  0.246 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

### Key Points from the Output:

Hop 1: Local Gateway

- 192.168.36.2 responded successfully.
- This is likely your router or virtual network gateway.

Hops 2–29: No Response

- All hops returned `\* \* \*`, meaning no ICMP or UDP replies were received.
- This suggests that intermediate routers or firewalls are \*\*blocking traceroute probes\*\*.

## No Final Destination Reached

- The target IP `160.46.226.165` did not respond.
- Could be due to:
- ICMP filtering
- Firewall restrictions
- Network segmentation or VPN

## TASK 16: GOOGLE DORKING

### APPROACH: Passive Reconnaissance

### TOOLS USED: Google

**Google Dorking, also known as Google Hacking, is the practice of using advanced Google search operators to find specific information—and often sensitive data—that is not readily available through a simple search. It's a form of "open-source intelligence" (OSINT).**

**By searching about BMW on google we got different portals like password management portal and B2B partner portal**

Google site:bmw.com X

All Mode All Images Short videos Videos Forums Web More ▾ Google promotion

**Try Google Search Console**  
www.google.com/webmasters/  
Do you own **bmw.com**? Get indexing and ranking data from Google.

 **bmw.com**  
<https://individual.bmw.com> :

**BMW M: Home of high performance cars**  
M. The most powerful letter in the world. **BMW M** has been a key player in the exceptional history of motorsport and stands for high-performance and passion ...

 **bmw.com**  
<https://www.bmw.com> > ... - Translate this page :

**BMW - официальный сайт в России**  
Оригинальные аксессуары для вашей семьи и вашего автомобиля **BMW**. Перейти в магазин.  
Выбор и покупка. Модельный ряд · Тест-драйв · Автомобили с пробегом · BMW ...

 **bmw.com**  
<https://www.bmw.com> > ... :

**Official BMW Malaysia website**  
Welcome to the official **BMW Malaysia** website: discover premium vehicle models, exclusive offers,

Google site:bmw.com "user" OR "password" X

All Mode All Images Videos Short videos News Forums More ▾

 **bmw.com**  
<https://xpita-b2b.bmw.com> > forgot-password :

**BMW B2X User Portal - Password Management**  
BMW B2X User Portal - **Password** Management. EN. BG. CN. CZ. DE. EN. FR. GR. HU. IT. JP ... Set **Password**. Search for identity by: Username. Username. Submit. An ...

 **Home - BMW Group Partner Portal - B2B Portal**  
<https://b2b.bmw.com> > web > password-reset :

**Passwort Reset - BMW Group Partner Portal**  
Click on the "Reset **password**" link. You will now be prompted to enter your **user** ID. · Select "Step 1" to get a time-limited (30 min) **password**. · After clicking on ...

 **BMW.com**  
<https://xpita-b2b.bmw.com> :

**BMW B2X User Portal - Password Management**  
Welcome to the **password** management system of the BMW Group. This system allows the **user**-friendly, automated and secure reset of your own **password** or the ...

 **BMW.com**  
<https://xpita-b2b.bmw.com> > set-password :

Google search results for "site:bmw.com "login"":

- BMW.com** https://bmw1solutionhk.bmw.com : **BMW1Solution Login**. User Name is required. Password is required. IWA Login Reset Password Login.
- BMW.com** https://securelogin.bmw.com > login : **Login**. Authenticator Enrollment Portal - Registration - Reset your PIN - Login.
- BMW.com** https://b2b.bmw.com : **Home - BMW Group Partner Portal - B2B Portal**. ... **Login**. Welcome. Portal Login - Register Password Management. Welcome. Our suppliers contribute directly to the success of the BMW Group. Together with our ...
- bmw.com** https://thecluboffice.bmw.com : **Login**. English. Join event or community or. **Login**. Use this if you have a talque account already.

## TASK 17: DNS & SUBDOMAIN DETAILS

### APPROACH Passive Reconnaissance

### TOOLS USED [dnsdumpster.com](https://dnsdumpster.com)

**System Locations**

**Hosting / Networks**

**Services / Banners**

Showing 50 records out of a total of 1737 found.

**A Records (subdomains from dataset)**

Host	IP	ASN	ASN Name	Open Services (from DB)	REV
24asc-int4.bmw.com	160.48.213.2	ASN 8590 11	BMW Bayerische Motoren Werke Aktiengesellschaft, DE Germany		2
72h-radar-int1.bmw.com	160.46.228.2	ASN 8590 13	BMW Bayerische Motoren Werke Aktiengesellschaft, DE		3

**An excel sheet is given below that is driven from the tool [dnsdumpster.com](https://dnsdumpster.com) it has the details of all the Subdomains there IP's and Open services.**

## **DNS\_details**

### **TASK 18: SEARCH EXPOSED DOCUMENTS OR CREDENTIALS USING GITHUB**

#### **APPROACH** Passive Reconnaissance

#### **TOOLS USED** GitHub

- The GitHub repository doesn't leak any immediate secrets, but may reveal strategic information helpful to a threat actor or penetration tester.
- **Tech Stack:** Primary use of Dart and Flutter for app development, with secondary use of TypeScript, Ruby, and native mobile languages (Objective-C, Java).

The screenshot shows the GitHub profile page for the organization 'bmw-tech'. The header includes the URL 'https://github.com/bmw-tech', a search bar, and navigation links for Overview, Repositories (6), Packages, and People (2). The main area features the BMW logo, the name 'BMW Tech', and the description 'BMW Open Source'. It shows 82 followers and links to the group website and email. A sidebar on the right displays popular repositories like 'ozzie.flutter', 'lumberdash', 'atlas', 'arb-converter-cli', and 'widget\_driver', along with sections for people, top languages (Dart, TypeScript), and most used topics (flutter, flutter-package). A 'Report abuse' link is also present.

https://github.com/bmw-tech/lumberdash

Code Issues Pull requests Actions Security Insights

**lumberdash** Public

Watch 9 Fork 24 Star 166

master Branches Tags

71 Commits

- .github
- art
- colorize\_lumberdash
- docs
- file\_lumberdash
- firebase\_lumberdash
- lumberdash
- print\_lumberdash
- sentry\_lumberdash
- .gitignore

About

Do you need logs? Lumberdash is the answer!

[pub.dartlang.org/packages/lumberdash](https://pub.dartlang.org/packages/lumberdash)

flutter flutter-package

Readme Activity Custom properties 166 stars 9 watching 24 forks Report repository

Releases 3 tags

https://github.com/bmw-tech/lumberdash

Code Issues 9 Pull requests 3 Actions Security Insights

**lumberdash** Public

Watch 9 Fork 24 Star 166

master Branch 3 Tags

Go to file

71 Commits

Author	Commit Message	Date
fabiomcarneiro	update sentry	6cb6387 · 4 years ago
.github	Add Automatic Publish Action (#73)	4 years ago
art	Upgrade plugins to support lumberdash v2 (#40)	6 years ago
colorize_lumberdash	[Update] Repository structure (#72)	4 years ago
docs	Revert docs folder rename	4 years ago
file_lumberdash	[Update] Repository structure (#72)	4 years ago
firebase_lumberdash	Add Automatic Publish Action (#73)	4 years ago
lumberdash	[Update] Repository structure (#72)	4 years ago
print_lumberdash	[Update] Repository structure (#72)	4 years ago
sentry_lumberdash	update sentry	4 years ago
.gitignore	Add Null Safety   Bump version 3.0.0   Update CI (#64)	4 years ago

About

Do you need logs? Lumberdash is the answer!

[pub.dartlang.org/packages/lumberdash](https://pub.dartlang.org/packages/lumberdash)

flutter flutter-package

Readme Activity Custom properties 166 stars 9 watching 24 forks Report repository

Releases 3 tags

The screenshot shows the GitHub repository page for `lumberdash`. The README section features a cartoon owl character wearing a lumberjack hat and holding a chainsaw, standing next to logs. Below the owl is a brief description: "Do you need logs? Lumberdash is the answer! With a simple but powerful logging API, Lumberdash is the easiest way to record logs. And if that is not enough, you can extend its API and create your own custom plugins for your own logging needs." The page also includes sections for "How it works", deployment history, and a language usage chart.

Language	Percentage
Dart	78.5%
Ruby	13.7%
Objective-C	3.6%
Java	2.2%
Other	2.0%

## TASK 19: REPORT MAKING

APPROACH: Passive Reconnaissance

TOOLS USED: shodan

This report shows that BMW.com is not a single server but a network of multiple hosts, primarily associated with BMW AG and other related organizations. The infrastructure is a mix of web servers (Apache, nginx, IIS) running on both Linux and Windows, with a strong emphasis on secure connections (TLS 1.2/1.3, HSTS).

# Shodan Report

bmw.com Total: 147

## // GENERAL

### Countries

Country	Count
Germany	87
China	29
United States	12
Netherlands	11
Australia	2

### Ports

Port	Count
443	133
80	13
5222	1

### Organization

Organization	Count
BMW AG	86
LONGTEL NETWORKS & TECHNOLOGIES LTD.	27
BMW Manufacturing Co., LLC	9
A100 ROW GmbH	6
Leaseweb Deutschland GmbH	5

[MORE...](#)

### Vulnerabilities

No information available.

### Products

Product	Count
Apache httpd	94
nginx	22
Microsoft IIS httpd	12

### Tags

Tag	Count
cloud	10
eol-product	2
starttls	1

### Operating Systems

Operating System	Count
Windows	12
Ubuntu	1

## // HTTP INSIGHTS

### Website Titles

Title	Count
BMW Group - no content deployed	18
Fleet Agent	11
404 Not Found	8
302 Found	7
403 - Forbidden: Access is denied.	7

[MORE...](#)

### Web Technologies

Technology	Count
HSTS	76
Apache HTTP Server	59
IIS	12
Nginx	11
Windows Server	11

[MORE...](#)

### Protocol Versions

Protocol Version	Count
http/1.1	7
h2	6

## // SSL INSIGHTS

### SSL/TLS Versions

Version	Count
tlsv1.2	132
tlsv1.3	97
tlsv1	1
tlsv1.1	1

### JARM Fingerprints

Fingerprint	Count
2ad2ad0002ad2ad00042d42d0000007d9a2df...	81
29d29d0000000000029d29d29d29d755f8...	22
29d29d00029d29d00029d29d29d29da8f16e8...	6
29d29d15d29d29d00041d41d00041da0568d6...	6
2ad2ad16d2ad2ad0002ad2ad2ad2ad6ec53d7...	3

[MORE...](#)

### JA3S Fingerprints

Fingerprint	Count
6c2811f7ba8e88604ea41a2bf9fa5ad7	86
303951d4c50efb2e991652225a6f02b1	22
134c270d52dd3495d39878f76f646581	8
03788d8896c247631764a250db971b74	6
ec74a5c51106f0419184d0dd08fb05bc	4

[MORE...](#)

## CASE STUDY OF RECENT DATA BREACH OF BMW

### **BMW FINANCIAL DATA BREACH 7 JULY 2015**

#### **Data breach at a vendor:**

The breach originated from a data security incident at AIS InfoSource, a third-party vendor that processes data for BMW Financial Services NA, LLC (BMW FS).

#### **Affected data:**

Customer personal data was exposed in the breach.

#### **Notification:**

BMW FS began notifying affected individuals and state authorities, including the New Hampshire and Texas Attorney Generals' offices, around July 3, 2025.

- The investigation is ongoing

## CONCLUSION

The OSINT and footprinting exercise on BMW.com shows how publicly available tools can reveal critical details such as domain records, technologies, IP addresses, subdomains, and security configurations without direct exploitation. While BMW demonstrates strong defenses with secure DNS, TLS, and CDN usage, findings like breached emails highlight the need for continuous monitoring. Overall, OSINT serves as both a potential attacker's entry point and a defender's tool for strengthening cybersecurity.

## References

OSINT Framework – <https://osintframework.com>

Wayback Machine – <https://archive.org/web/>

Whois Lookup – <https://whois.domaintools.com>

BuiltWith – <https://builtwith.com>

Wappalyzer – <https://www.wappalyzer.com>

Have I Been Pwned – <https://haveibeenpwned.com>

Shodan – <https://www.shodan.io>

ipinfo.io – <https://ipinfo.io>

## **Tools Used**

WHOIS Lookup → Domain registration details

Have I Been Pwned / Security Headers → Breach check

BuiltWith & Wappalyzer → Technology stack analysis

Wayback Machine → Historical snapshots of BMW.com

dig → DNS queries

ipinfo.io → IP and ASN details

Sublist3r → Subdomain enumeration

nmap → Port scanning and service detection

nslookup → IP address resolution

theHarvester → Email & subdomain collection

dnsenum → DNS enumeration, MX records, zone transfer attempts

ssllscan → SSL/TLS configuration check

Sherlock → Username enumeration on social media & platforms

SpiderFoot → OSINT visualization and data correlation

traceroute → Network path tracing

Shodan → Host and service discovery across the internet

**Note :**

**Active Reconnaissance** interacts with a target's systems through techniques like port scanning to uncover detailed information, but it carries a high risk of detection.

**Passive reconnaissance**, conversely, gathers information from publicly available sources, such as social media and DNS records, without any direct interaction, making it much stealthier and less detectable.