INFORMATION GATHERING REPORT

MONICA LICEA CASTRO
RABRIAL, S.A.

TABLE OF CONTENTS

In the field of cybersecurity, information gathering is a crucial phase in assessing the security posture of a target. This phase involves collecting publicly available data about a domain to understand its infrastructure, potential vulnerabilities, and security measures.

For this report, the chosen target is TomTom.com, the official website of TomTom N.V., a global company specializing in location technology and digital mapping. Founded in 1991 and headquartered in the Netherlands, TomTom is widely known for its GPS navigation devices, real-time traffic information, and mapping solutions. Over the years, it has expanded into advanced driver assistance systems (ADAS), autonomous driving, and geospatial data services for businesses.

By analyzing **TomTom.com**, this report aims to apply **information gathering techniques** to identify public-facing assets, subdomains, IP addresses, and other relevant cybersecurity aspects.

I intentionally selected **TomTom.com** as the target for this exercise because I have been very familiar with its products and a personal fan of its technology since the 90s. This familiarity provides an added layer of interest and motivation in conducting a thorough analysis while ensuring that all information gathering remains within ethical and legal boundaries.

VERTICAL FOOTPRINTING

I will be using the following tools; however not all tools will provide results: DNS Brute Force (shuffledns), Google Analytics (Analytics Relationships), TLS Probing (Cero), Web Scraping (Katana), Certificate Transparency Logs (ctfr), Web Files/Cache (gau), Link Results and execute permutations (alterx + dnsx), and Group all subdomains found. **From hackerone.com, I have selected tomtom.com.**

Offers bounties
High response efficiency
Managed by HackerOne
Offers retesting

Program	Launch date	Reports resolved	Bounties minimum	Bounties average
TomTom Managed	11 / 2024	47	-	-

Asset name	Type	Coverage	Max. severity	Bounty	Last update	Resolved Reports
*.tomtom-global.com	Wildcard	In scope	Critical	Ineligible	Mar 28, 2024	5 (11%)
*.tomtomgroup.com	Wildcard	In scope	Critical	Ineligible	Mar 28, 2024	20 (43%)
*.tomtom.com	Wildcard	In scope	Critical	Ineligible	Mar 28, 2024	20 (43%)

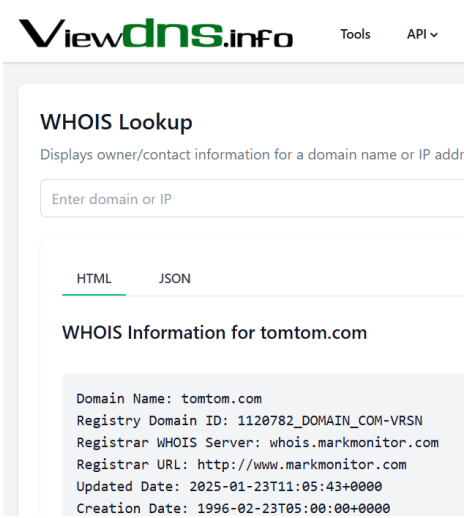
I start by reviewing the VIEW DNS RECORD

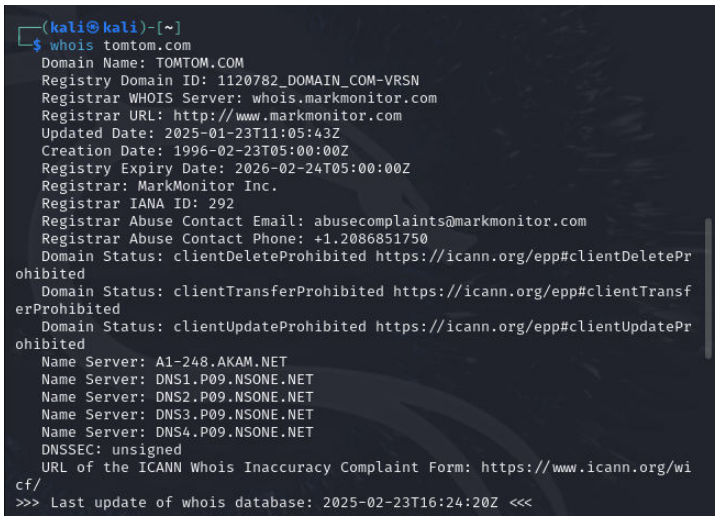
https://viewdns.info/dnsrecord/?domain=tomtom.com

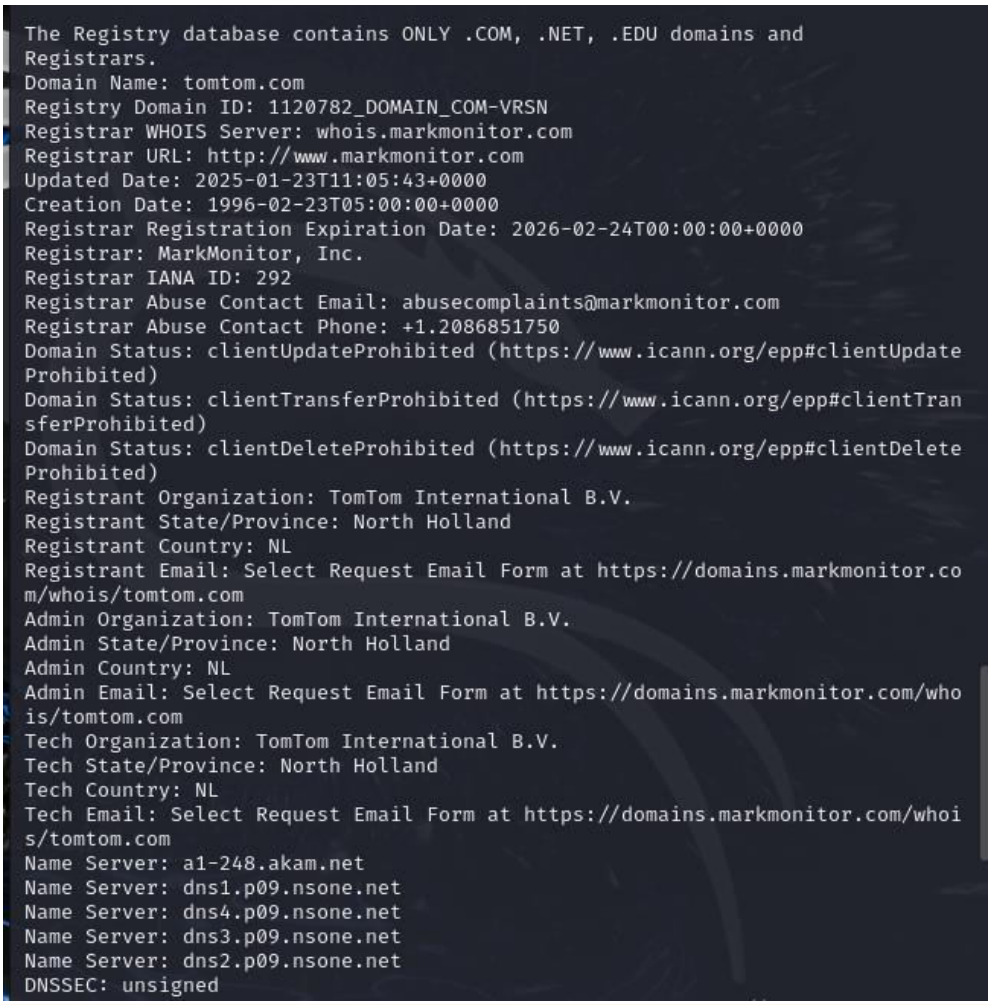
Please access this file or the link above:

tomtom.com DNS Records - ViewDNS.info.pdf

I also verified tomtom.com with WHOIS







Key findings:

Domain Registration Information

- Domain Name: tomtom.com
- Registry Domain ID: 1120782_DOMAIN_COM-VRSN
- Registrar: MarkMonitor Inc. (A domain management company that protects corporate domains)
- Registrar WHOIS Server: whois.markmonitor.com
- Registrar URL: MarkMonitor
- Creation Date: 1996-02-23
- Updated Date: 2025-01-23
- Expiration Date: 2026-02-24

Domain Status Codes: The domain has multiple EPP Status Codes: clientDeleteProhibited, which prevents deletion of the domain, clientTransferProhibited, which prevents transfer to another registrar, and clientUpdateProhibited, which prevents modifications to domain details.

These statuses indicate that TomTom has locked the domain for security to prevent unauthorized changes or takeovers.

Registrant and Admin Contact

- Registrant Organization: TomTom International B.V.
- Registrant Location: North Holland, Netherlands (NL)
- Admin and Tech Contact: Also, TomTom International B.V.
- Email Contacts: Hidden via MarkMonitor's privacy service.

Since the registrant is TomTom International B.V., this confirms it is owned by the official company behind TomTom navigation devices.

Name Servers (DNS): TomTom uses Akamai and NSOne DNS services for domain resolution:

- A1-248.AKAM.NET
- DNS1.P09.NSONE.NET
- DNS2.P09.NSONE.NET
- DNS3.P09.NSONE.NET
- DNS4.P09.NSONE.NET

Akamai provides DDoS protection and content delivery, while NSOne is a high-performance DNS provider. This suggests TomTom has a strong infrastructure for uptime and security.

DNS Security Extensions (DNSSEC): DNSSEC Status: unsigned. TomTom has not enabled DNSSEC, meaning DNS records are not cryptographically signed to prevent tampering.

Additional Information: The whois data was last updated on March 1, 2025, so the information is fresh. The domain has been registered since 1996, making it one of the older domains on the internet.

Key Takeaways

- TomTom International B.V. officially owns and controls the domain.
- The domain is highly protected (locked against transfers, updates, and deletions).
- It is using Akamai and NSOne for high-performance DNS resolution.
- No personal contact details are exposed due to GDPR and MarkMonitor privacy protection.
- DNSSEC is not enabled, which could be a potential security improvement.

I ran the nslookup, dig, and host commands for DNS queries. They helped me to gather information about domain names, IP addresses, and other DNS records. With nslookup, I can retrieve IP addresses, mail servers, name servers, and other DNS records.

```
┌──(kali㉿kali)-[~]
└─$ host tomtom.com
nslookup tomtom.com
dig +short tomtom.com

tomtom.com has address 98.64.11.144
tomtom.com mail is handled by 10 tomtom-com.mail.protection.outlook.com.
;; communications error to 100.100.1.1#53: timed out
Server:         100.100.1.1
Address:        100.100.1.1#53

Non-authoritative answer:
Name:   tomtom.com
Address: 98.64.11.144

98.64.11.144
```

Using **bgp.he.net** I was able to locate the **ASN** from **tomtom.com**.

Result	Type	Description
AS49838	ASN	TomTom International B.V.

HURRICANE ELECTRIC INTERNET SERVICES

Search

AS49838 TomTom International B.V.

Quick Links | AS Info | Graph v4 | Prefixes v4 | Peers v4 | Whois | RDAP | IRR | Traceroute

BGP Toolkit Home
BGP Prefix Report
BGP Peer Report
Super Traceroute
Super Looking Glass
Exchange Report
Bogon Routes
World Report

Prefix	Description	Visibility
185.5.120.0/22	TomTom International B.V.	100% 652/652
185.5.121.0/24	TomTom International B.V.	100% 652/652
185.5.122.0/24	TomTom International B.V.	100% 652/652
185.5.123.0/24	TomTom International B.V.	100% 652/652

Showing 1-4 of 4

With tomtom.com's ASN, I was able to retrieve IP address blocks associated with this Autonomous System Number (ASN), IP address ranges that belong to this ASN, useful information for cybersecurity, penetration testing, and network analysis, such as mapping an organization's infrastructure or an internet provider's IP space.

```
┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ whois -h whois.radb.net   -- '-i origin AS49838' | grep -Eo "([0-9.]+){4}/[0-9]+" | uniq > whois.txt

┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ cat whois.txt
185.5.120.0/22
185.5.120.0/24
185.5.121.0/24
185.5.122.0/24
185.5.123.0/24
```

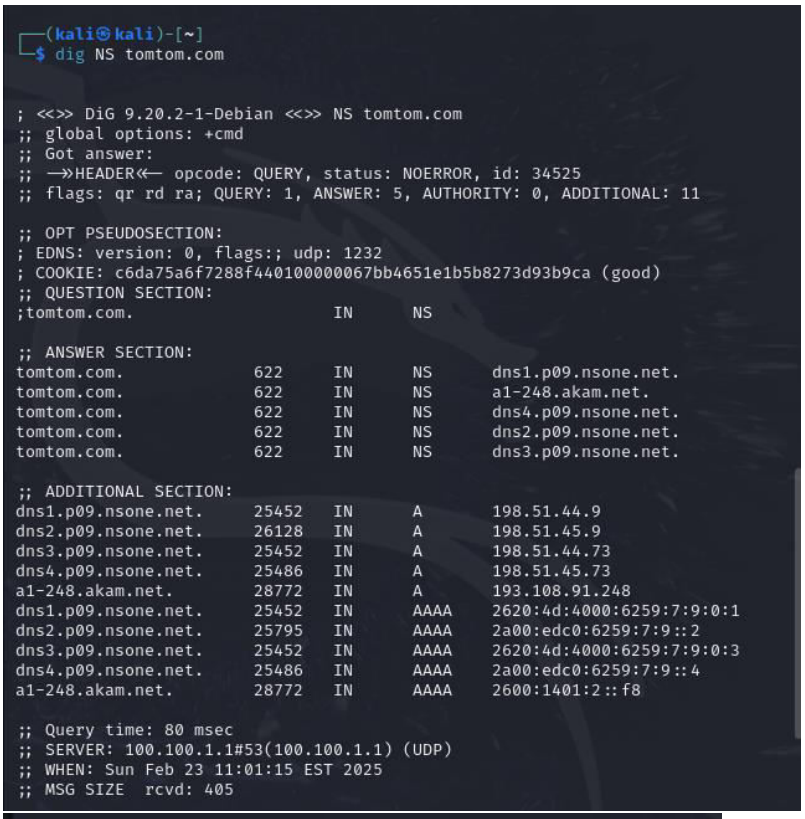
The dig command returns the A record (IPv4 address) for tomtom.com.

```
┌──(kali㉿kali)-[~]
└─$ dig ANY tomtom.com


; <<>> DiG 9.18.16-1-Debian <<>> ANY tomtom.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21871
;; flags: qr rd ra; QUERY: 1, ANSWER: 36, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 96d4dd736e9b85cf0100000067b092067eb9e03993d0161a (good)
;; QUESTION SECTION:
;tomtom.com.                    IN      ANY

;; ANSWER SECTION:
tomtom.com.             3600    IN      SOA     dns1.p09.nsone.net. hostmaster.nsone.net. 1648553945 7200 3600 24796800 3600
tomtom.com.             3600    IN      TXT     "miro-verification=c366a88d6ef9552f4a93d9016e5eb3b8ec5d47bb"
tomtom.com.             3600    IN      TXT     "docusign=4e2ef447-c398-49eb-885f-93a3c38cb230"
tomtom.com.             3600    IN      TXT     "b3hqxdn8mym6085y5qjjmglycyytzvgf"
tomtom.com.             3600    IN      TXT     "teamviewer-sso-verification=d61bf8d9f45847469ee7545563807b70"
tomtom.com.             3600    IN      TXT     "MS=ms14080619"
tomtom.com.             3600    IN      TXT     "google-site-verification=UzHGW9mOc94-x3sIA1aH0UDc2t8EGPIWewIT72bMVBM"
tomtom.com.             3600    IN      TXT     "adobe-idp-site-verification=a0c9aec7-2cac-4280-b67d-87c4a648f73b"
tomtom.com.             3600    IN      TXT     "docusign=3ce7bb6d-7e84-47a7-8d4f-dcd7de13f634"
tomtom.com.             3600    IN      TXT     "apple-domain-verification=NAGVDc5TxR8AvHUb"
tomtom.com.             3600    IN      TXT     "onetrust-domain-verification=829e27e3ec234967a16cbe0f3bae485c"
tomtom.com.             3600    IN      TXT     "onetrust-domain-verification=ed9b028f470a4f418effe0bb8faf3af8"
tomtom.com.             3600    IN      TXT     "google-site-verification=AIX2eLQtiGKMjrdTkaNIjlibc69ZhosNZEQU4XvvDPY"
tomtom.com.             3600    IN      TXT     "RV = QuoVadis=b7857c09-11e4-4c65-8a10-df1305b6642a"
tomtom.com.             3600    IN      TXT     "ms-domain-verification=5808bf5a-1792-495f-b5f1-e33e1cf1390c"
tomtom.com.             3600    IN      TXT     "h1-domain-verification=9cZmw66YqZ1Nb3DAMtPQYPRurXKQ3kgX7KTT8ypD1NU1WxC2"
tomtom.com.             3600    IN      TXT     "identrust_validate=hdIpSbx0ykv6XbCNUp2sUzubdfTombetgZYOY4GgqG3M"
tomtom.com.             3600    IN      TXT     "google-site-verification=WO42AZ7OcwAQhtl5RmaR0dlngJYc0bqbypY3bhH6XbM"
tomtom.com.             3600    IN      TXT     "v=spf1 include:spf.protection.outlook.com include:sharepointonline.com include:_spf.salesforce.com ip4:20.76.56.69 -all"
tomtom.com.             3600    IN      TXT     "mixpanel-domain-verify=4b828da3-f72e-4fa9-b096-6b8bd90bcbe0"
tomtom.com.             3600    IN      TXT     "pardot510681=40442bb65425b211ae9d2d6de714659b41600748d54e1e6ac7faeed415190f48"
tomtom.com.             3600    IN      TXT     "S+J8Uhi6PW4nuHLLTx5XJGX8/4Uwh7QiFB1TIGFgrYkkEXHcG0IYkEU/xiZ0064EnxtaOuzKM8PMFJPTckzAOg=="
tomtom.com.             3600    IN      TXT     "google-site-verification=GzfIXCzElSCZaGP3KID04CgZ-JIxTa2KDF5kOPiuxbE"
tomtom.com.             3600    IN      TXT     "atlassian-domain-verification=LNTzFCPe79DXpAt4NY1pKp5ZNIuZFPoQQ00EHwKjcQX1W0QLQDEDLEftCwNPoaJc"
tomtom.com.             3600    IN      TXT     "facebook-domain-verification=cpwht607889mbpsxlzqbrtvmmgwm93"
tomtom.com.             3600    IN      TXT     "docker-verification=2158b838-492e-404d-90c3-21764f1c446e"
tomtom.com.             3600    IN      TXT     "google-site-verification=fY7o80hMancXdF59CPD2XUPr5ck9JySV-jwgufbHbVE"
tomtom.com.             3600    IN      TXT     "hcp-domain-verification=865afc456cf26f92967c598d0c27a913040e4e23b8167e02f022db1a3bc929c1"
tomtom.com.             3600    IN      TXT     "90e4ae7308c543e59bc45ad2c7c0c6ba"
tomtom.com.             3600    IN      MX      10 tomtom-com.mail.protection.outlook.com.
tomtom.com.             208     IN      A       98.64.11.144
tomtom.com.             9145    IN      NS      dns4.p09.nsone.net.
tomtom.com.             9145    IN      NS      dns1.p09.nsone.net.
tomtom.com.             9145    IN      NS      dns2.p09.nsone.net.
tomtom.com.             9145    IN      NS      dns3.p09.nsone.net.
tomtom.com.             9145    IN      NS      a1-248.akam.net.

;; Query time: 16 msec
;; SERVER: 100.100.1.1#53(100.100.1.1) (TCP)
;; WHEN: Sat Feb 15 08:09:24 EST 2025
;; MSG SIZE  rcvd: 2411
```

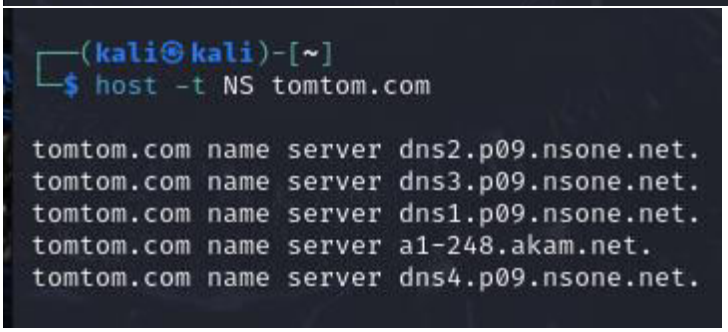
This command returns the mail servers for tomtom.com.

```
File  Actions  Edit  View  Help
└─$ dig MX tomtom.com


; <<>> DiG 9.20.2-1-Debian <<>> MX tomtom.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33867
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 6f0af11d01f326370100000067bb45feff319cbb9d6800be (good)
;; QUESTION SECTION:
;tomtom.com.                    IN      MX

;; ANSWER SECTION:
tomtom.com.             2768    IN      MX      10 tomtom-com.mail.protection
.outlook.com.

;; Query time: 100 msec
;; SERVER: 100.100.1.1#53(100.100.1.1) (UDP)
;; WHEN: Sun Feb 23 10:59:52 EST 2025
;; MSG SIZE  rcvd: 121
```

These comands return the **name servers** handling tomtom.com



```
┌──(kali㉿kali)-[~]
└─$ dig NS tomtom.com

; <<>> DiG 9.20.2-1-Debian <<>> NS tomtom.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34525
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 11

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: c6da75a6f7288f440100000067bb4651e1b5b8273d93b9ca (good)
;; QUESTION SECTION:
;tomtom.com.                    IN      NS

;; ANSWER SECTION:
tomtom.com.             622     IN      NS      dns1.p09.nsone.net.
tomtom.com.             622     IN      NS      a1-248.akam.net.
tomtom.com.             622     IN      NS      dns4.p09.nsone.net.
tomtom.com.             622     IN      NS      dns2.p09.nsone.net.
tomtom.com.             622     IN      NS      dns3.p09.nsone.net.

;; ADDITIONAL SECTION:
dns1.p09.nsone.net.     25452   IN      A       198.51.44.9
dns2.p09.nsone.net.     26128   IN      A       198.51.45.9
dns3.p09.nsone.net.     25452   IN      A       198.51.44.73
dns4.p09.nsone.net.     25486   IN      A       198.51.45.73
a1-248.akam.net.        28772   IN      A       193.108.91.248
dns1.p09.nsone.net.     25452   IN      AAAA    2620:4d:4000:6259:7:9:0:1
dns2.p09.nsone.net.     25795   IN      AAAA    2a00:edc0:6259:7:9::2
dns3.p09.nsone.net.     25452   IN      AAAA    2620:4d:4000:6259:7:9:0:3
dns4.p09.nsone.net.     25486   IN      AAAA    2a00:edc0:6259:7:9::4
a1-248.akam.net.        28772   IN      AAAA    2600:1401:2::f8

;; Query time: 80 msec
;; SERVER: 100.100.1.1#53(100.100.1.1) (UDP)
;; WHEN: Sun Feb 23 11:01:15 EST 2025
;; MSG SIZE  rcvd: 405
```



```
┌──(kali㉿kali)-[~]
└─$ host -t NS tomtom.com

tomtom.com name server dns2.p09.nsone.net.
tomtom.com name server dns3.p09.nsone.net.
tomtom.com name server dns1.p09.nsone.net.
tomtom.com name server a1-248.akam.net.
tomtom.com name server dns4.p09.nsone.net.
```

I performed a Reverse DNS lookup, which you can review by accessing the link, or the PDF file right below.

Reverse DNS lookup

https://viewdns.info/reversewhois/?q=tomtom.com&t=1

Please access this file or the link above:

tomtom.com - Reverse Whois Lookup - ViewDNS.info.pdf

I used the Reverse WHOIS Search tool from WHOISXMLAPI to find all domain names registered with a particular email address, name, phone number, or other registrant details.

Please access this file: Reverse-WHOIS-DRS-report-tomtom.com.c

The Full-Text Search tool on the RIPE Database allowed me to perform detailed searches across the RIPE NCC database. The database holds information related to IP address allocations, Autonomous System Numbers (ASNs), and Internet resources in the European, Middle Eastern, and part of Central Asia regions.

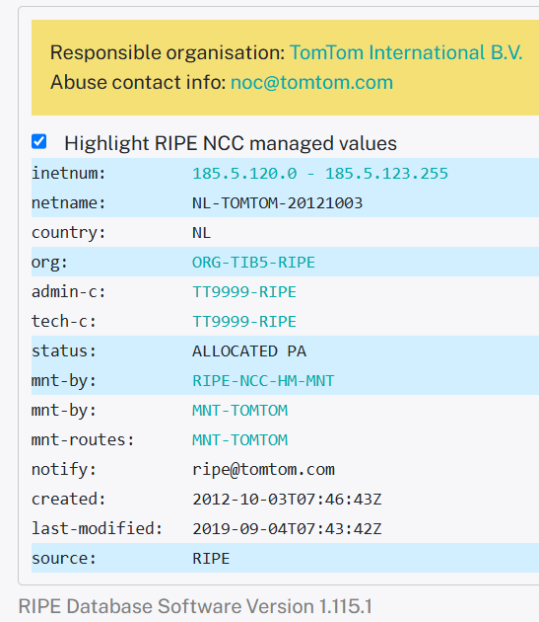
With this tool I was able to find IP address allocations, Autonomous System Numbers (ASNs), contact Information, Routing Information

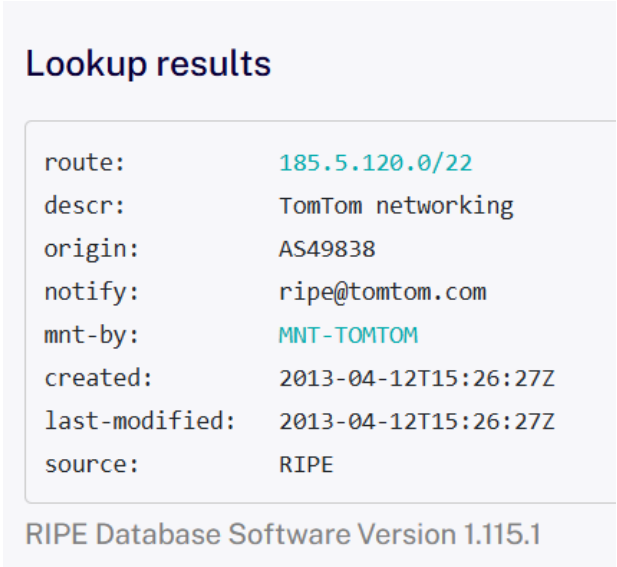
https://apps.db.ripe.net/db-web-ui/fulltextsearch

For example:

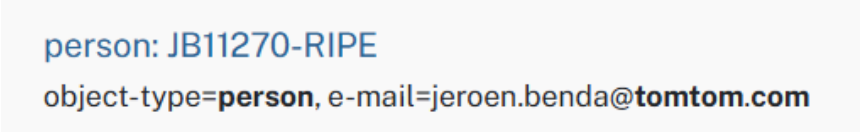
inetnum: 185.5.120.0 - 185.5.123.255,
notify=ripe@**tomtom.com**

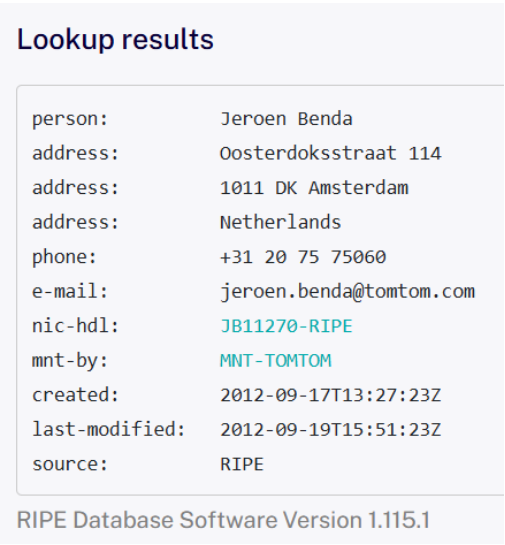
route: 185.5.120.0/22AS49838
notify=ripe@tomtom.com





And





I now run the following command: dnsvalidator.

```
┌──(kali㉿vbox)-[~/recopilacion/lists]
└─$ dnsvalidator -tL https://raw.githubusercontent.com/blechschmidt/massdns/master/lists/resolvers.txt -threads 100 -o $HOME/recopilacion/lists/resolvers.txt
═══════════════════════════════════════════════════
dnsvalidator v0.1       by James McLean (@vortexau)
                        & Michael Skelton (@codingo_)
═══════════════════════════════════════════════════
[14:53:57] [INFO] [1.1.1.1] resolving baseline
[14:53:57] [INFO] [8.8.8.8] resolving baseline
[14:53:57] [INFO] [173.223.98.69] Checking ...
[14:53:57] [INFO] [8.26.56.143] Checking ...
[14:53:57] [INFO] [8.29.3.139] Checking ...
[14:53:57] [INFO] [119.201.155.78] Checking ...
```

```
[15:28:15] [ERROR] [91.190.230.150] Error when checking NXDOMAIN, passing
[15:28:16] [ERROR] [5.175.46.61] Error when checking NXDOMAIN, passing
[15:28:16] [INFO] Finished. Discovered 2484 servers
```

```
┌──(kali㉿kali)-[~/recopilacion/lists/tomtom.com/0211]
└─$ cat resolvers.txt | wc
    307     307    4174
```

I obtained a file containing only the valid DNS resolvers from the provided list, making it useful for DNS testing or creating a refined list of working resolvers. With this file, I downloaded a list of DNS resolvers from the given GitHub URL which contains publicly available DNS servers, I validated each resolver from the list to check if it's working correctly and can resolve domain names, the command used 100 threads to speed up the validation process by testing multiple resolvers simultaneously, and I saved the list of valid resolvers to the specified file: $HOME/recopilacion/lists/tomtom.com.0211/resolvers.txt. Please access the file resolvers.txt for the complete list.

Google Analytics did not turn up any results.

```
┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ analyticsrelationships --url https://www.tomtom.com/
```

```
[+] Analyzing url: https://www.tomtom.com/
[-] Tagmanager URL not fount
```

```
┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ cat analytics.txt | wc
      0       0       0
```

TLS Probing using ***cero***. With this tool I was able to find the domain information, subdomains, among other info.

```
┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ cero -d tomtom.com
url-redirector-prod.tomtomgroup.com
tomtom.fi
tomtom.nl
openlr.org
tomtom.com
ttcode.com
tomtommaps.com
www.ttcode.com
beat.tomtom.com
tomtomgroup.com
tomtomplaces.com
engage.tomtom.com
groups.tomtom.com
intouch.tomtom.com
it.tomtomgroup.com
sd.tomtomgroup.com
thebeat.tomtom.com
devforum.tomtom.com
edp.tomtomgroup.com
hrsd.tomtomgroup.com
itsd.tomtomgroup.com
office365.tomtom.com
onboarder.tomtom.com
orbisps.tomtomgroup.com
feedback.tomtomgroup.com
security.tomtomgroup.com
itsupport.tomtomgroup.com
```

With the subfinder command, I was able to find tomtom.com's subdomains. They are included in the file: **subfinder.txt.**

```
┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ subfinder -d tomtom.com -o subfinder.txt -silent
```

```
┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ cat subfinder.txt | wc
   2540    2540   93963
```

The file **targets.txt** contains the IP lots.

```
┌──(kali㉿kali)-[~]
└─$ subfinder -d tomtom.com | tee targets.txt
```

```
┌──(kali㉿kali)-[~/recopilacion/lists/tomtom.com/0211]
└─$ cat targets.txt
185.5.120.0/22
185.5.120.0/24
185.5.121.0/24
185.5.122.0/24
185.5.123.0/24
```

```
┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ cat targets.txt | wc
   2544    2544   94176
```

Web Scraping technique only for the main domain, it can also be performed against all subdomains. The commands used were katana for the scraping and unfurl to extract URL's domain.

```
┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ echo tomtom.com | katana -jc -o katanaoutput.txt -kf robotstxt,sitemapxml
```

```
┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ cat tt_katana.txt | wc
   1280    1280  115608
```

```
┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ cat katanaoutput.txt | unfurl --unique domains > katana.txt

┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ cat katana.txt
www.tomtom.com
developer.tomtom.com
help.tomtom.com
media.tomtom.com
move.tomtom.com
corporate.tomtom.com
mapmaker.tomtom.com
support.move.tomtom.com
download.tomtom.com
status.tomtom.com
www-preprod.tomtom.com
tomtom.com

┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ cat katana.txt | wc
     12      12     222
```

Here's a breakdown of what each of these TomTom subdomains is likely to be used for, based on the naming conventions:

1. **www.tomtom.com**: The main website for TomTom, which likely includes general product information, services, and company details.
2. **developer.tomtom.com**: A portal dedicated to developers. This is where TomTom provides resources, tools, and APIs for developers who want to integrate TomTom services like maps, navigation, and traffic data into their own applications.
3. **help.tomtom.com**: The support or help section for TomTom customers. It likely contains user guides, FAQs, troubleshooting, and other resources to assist users with TomTom products.
4. **media.tomtom.com**: A section for media and press releases, where TomTom provides news, press kits, images, and other materials for journalists and media outlets.
5. **move.tomtom.com**: Likely related to TomTom's products or services in the mobility or transportation sector. This could include services for fleet management, vehicle navigation, or business solutions involving location-based technology.
6. **corporate.tomtom.com**: A subdomain dedicated to corporate information. This could include investor relations, company reports, corporate announcements, and other business-related content.
7. **mapmaker.tomtom.com**: This likely refers to TomTom's mapping services. Map Maker could be a tool or platform for users to contribute to or edit TomTom's maps, similar to other map-editing platforms.

8. **support.move.tomtom.com**: A support portal specifically for users of TomTom's mobility-related services (such as fleet management or navigation for businesses).
9. **download.tomtom.com**: A subdomain used for downloading TomTom software, such as map updates, firmware updates, or applications for their devices.
10. **status.tomtom.com**: A page that provides real-time information about the status of TomTom's services, including operational status, outages, or planned maintenance.
11. **www-preprod.tomtom.com**: This could be a pre-production or staging version of TomTom's main website. It's likely used for testing and development before new updates or features go live on the main site.

Each of these subdomains appears to serve a specific function related to different aspects of TomTom's products, services, and customer engagement.

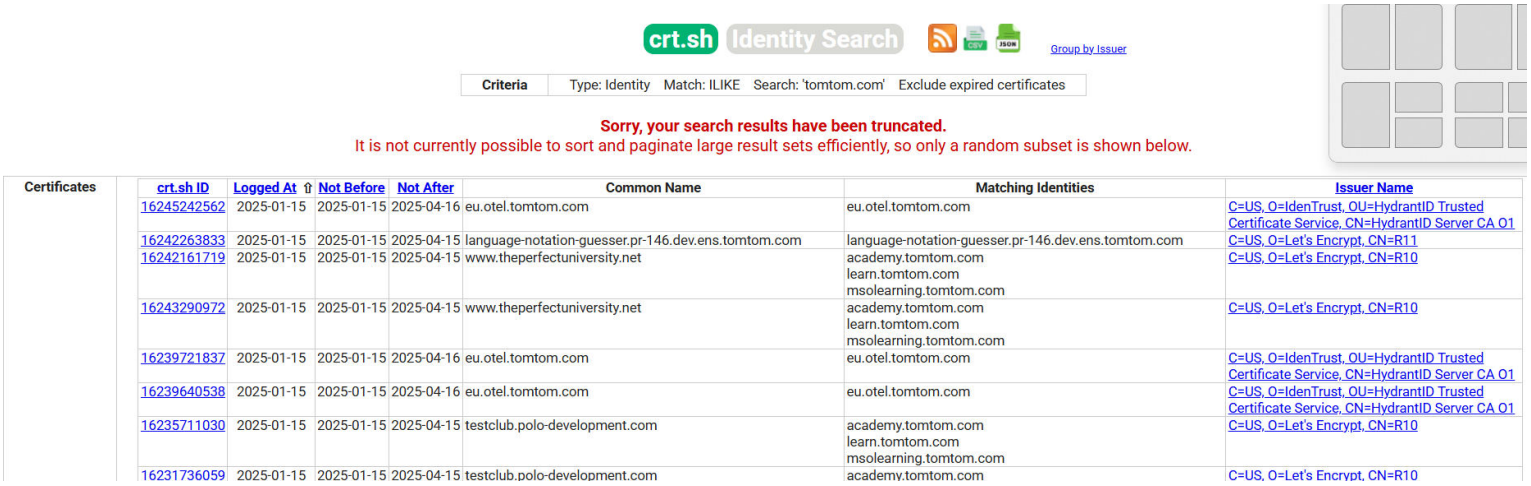
Everything is included in the following file: **subdominios.txt**

```
┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ cat shuffledns.txt analytics.txt cero.txt katana.txt > subdominios.txt

┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ cat subdominios.txt | wc
     39      39     726
```

I consulted the ***Certificate Transparency Logs*** to use these logs to search associated subdomains and to find the generated SSL certificate for tomtom.

https://crt.sh/

This is a short sample of the output on crt.sh. The complete list in the following file:


crt.sh Identity Search Group by Issuer

Criteria	Type: Identity Match: ILIKE Search: 'tomtom.com' Exclude expired certificates

Sorry, your search results have been truncated.
It is not currently possible to sort and paginate large result sets efficiently, so only a random subset is shown below.

Certificates	crt.sh ID	Logged At ⇧	Not Before	Not After	Common Name	Matching Identities	Issuer Name
	16245242562	2025-01-15	2025-01-15	2025-04-16	eu.otel.tomtom.com	eu.otel.tomtom.com	C=US, O=IdenTrust, OU=HydrantID Trusted Certificate Service, CN=HydrantID Server CA O1
	16242263833	2025-01-15	2025-01-15	2025-04-15	language-notation-guesser.pr-146.dev.ens.tomtom.com	language-notation-guesser.pr-146.dev.ens.tomtom.com	C=US, O=Let's Encrypt, CN=R11
	16242161719	2025-01-15	2025-01-15	2025-04-15	www.theperfectuniversity.net	academy.tomtom.com learn.tomtom.com msolearning.tomtom.com	C=US, O=Let's Encrypt, CN=R10
	16243290972	2025-01-15	2025-01-15	2025-04-15	www.theperfectuniversity.net	academy.tomtom.com learn.tomtom.com msolearning.tomtom.com	C=US, O=Let's Encrypt, CN=R10
	16239721837	2025-01-15	2025-01-15	2025-04-16	eu.otel.tomtom.com	eu.otel.tomtom.com	C=US, O=IdenTrust, OU=HydrantID Trusted Certificate Service, CN=HydrantID Server CA O1
	16239640538	2025-01-15	2025-01-15	2025-04-16	eu.otel.tomtom.com	eu.otel.tomtom.com	C=US, O=IdenTrust, OU=HydrantID Trusted Certificate Service, CN=HydrantID Server CA O1
	16235711030	2025-01-15	2025-01-15	2025-04-15	testclub.polo-development.com	academy.tomtom.com learn.tomtom.com msolearning.tomtom.com	C=US, O=Let's Encrypt, CN=R10
	16231736059	2025-01-15	2025-01-15	2025-04-15	testclub.polo-development.com	academy.tomtom.com	C=US, O=Let's Encrypt, CN=R10

I used the ctfr tool for subdomain enumeration and querying Certificate Transparency (CT) logs. I used it to search for subdomains for tomtom.com that have been issued SSL/TLS certificates. The subdomains are available By accessing the file: ctfr.txt.

```
┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ ctfr -d tomtom.com > ctfr.txt
```

```
┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ cat ctfr.txt | wc
   2542    3615   75340
```

```
┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ cat ctfr.txt | unfurl --unique domains > ctfr_limpio.txt

┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ cat ctfr_limpio.txt | wc
    813     813   23129
```

Web and Cache Files

I used the gau command to collect historical and live URLs for a given domain by scraping various sources. The results can be found in the file: gauoutput.txt.

```
┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ gau --threads 5 tomtom.com --o gauoutput.txt
WARN[0000] error reading config: Config file /home/kali/.gau.toml not found, using
default config

┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ cat gauoutput.txt | wc
 610302  610303 63707604
```

I proceeded with this command to extract only domain names for tomtom.com, not full URLs., to remove duplicates for a clean list, for subdomain enumeration and filtering unnecessary data.

```
┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ cat gauoutput.txt | unfurl --unique domains > gau.txt
```

```
┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ cat gau.txt | wc
    271     271    6705
```

I used bruteforce with shuffledns to try to find tomtom.com's subdomains.

```
┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ shuffledns -mode bruteforce -d tomtom.com -w $HOME/recopilacion/lists/domains.txt -r $HOME/recopilacion/lists/resolvers.txt -silent > shuffledns.txt
```

I didn't find anything with this tool.

```
┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ cat shuffledns.txt

┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ cat shuffledns.txt | wc
       0       0       0
```

The permutation technique was used to try to increase the list of targets.

```
┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ cat subdominios.txt | alterx | dnsx -o alterx.txt
```

```
┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ cat alterx.txt | wc
     97      97    2148
```

FINGERPRINTING

For the Fingerprinting phase, I will be using several tools to identify and collect specific details about tomtom's system, network, or application, to understand the underlying technologies, versions, configurations, and potential vulnerabilities. I will be performing active and passive fingerprinting. For the active phase, I will be interacting with tomtom's system by sending probes and requests to gather information. Although this method is more detectable by security systems, such as firewalls and IDS/IPS, I can find OS, open ports, services (using nmap), I can identify web technologies and CMS with whatweb and identify Web Application Firewalls with wafwoof. During the passive phase, I will observe traffic without directly interacting with the target system. I like this method because it is stealthier since it relies on analyzing logs, metadata, and leaked information. I will be using whois lookup to find the tomtom's domain registration info; dig and host to find subdomains, MX and NS records, and TheHarvester to try to extract emails, IPs and leaks.
I will be looking for information, such as OS, I will be using nmap, whatweb, wappalyzer and masscan. Fingerprinting is a critical part of information gathering because it helps penetration testers map out the target's surface, allows defenders to identify weaknesses before attackers do, provides context for selecting the right attack vectors and supports red teaming, OSINT, and vulnerability assessments.

- Scanning ports and detecting services with nmap

```
┌──(kali㉿kali)-[~/recopilacion/lists/tomtom.com/0211]
└─$ sudo nmap -Pn -sS -sV -p 0-65535 tomtom.com

Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-15 07:56 EST
Stats: 0:10:36 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 84.93% done; ETC: 08:08 (0:01:51 remaining)
Verbosity Increased to 1.
Stats: 0:10:36 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 84.94% done; ETC: 08:08 (0:01:51 remaining)
SYN Stealth Scan Timing: About 90.35% done; ETC: 08:09 (0:01:13 remaining)
SYN Stealth Scan Timing: About 95.58% done; ETC: 08:09 (0:00:34 remaining)
Completed SYN Stealth Scan at 08:09, 788.38s elapsed (65536 total ports)
Initiating Service scan at 08:09
Scanning 2 services on tomtom.com (98.64.11.144)
Completed Service scan at 08:09, 12.34s elapsed (2 services on 1 host)
NSE: Script scanning 98.64.11.144.
Initiating NSE at 08:09
Completed NSE at 08:09, 0.62s elapsed
Initiating NSE at 08:09
Completed NSE at 08:09, 0.42s elapsed
Nmap scan report for tomtom.com (98.64.11.144)
Host is up (0.050s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Microsoft Azure Application Gateway v2
443/tcp open  ssl/http Microsoft Azure Application Gateway v2

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 813.03 seconds
           Raw packets sent: 131669 (5.793MB) | Rcvd: 534 (23.496KB)
```

```
┌──(kali㉿kali)-[~/recopilacion/lists/tomtom.com/0211]
└─$ sudo nmap -Pn -sS -sV -p 443 tomtom.com

Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-15 07:53 EST
Nmap scan report for tomtom.com (98.64.11.144)
Host is up (0.050s latency).

PORT    STATE SERVICE  VERSION
443/tcp open  ssl/http Microsoft Azure Application Gateway v2

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.56 seconds
```

```
┌──(kali㉿kali)-[~/recopilacion/lists/tomtom.com/0211]
└─$ sudo nmap -sn -iL targets.txt
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-15 07:15 EST
Nmap scan report for 185.5.123.254
Host is up (0.055s latency).
Nmap done: 2048 IP addresses (1 host up) scanned in 656.05 seconds
```

Nmap with **nmapoutput.txt** file

```
┌──(kali㉿kali)-[~/recopilacion/lists/tomtom.com/0211]
└─$ sudo nmap -sn -iL targets.txt > nmapoutput.txt

┌──(kali㉿kali)-[~/recopilacion/lists/tomtom.com/0211]
└─$ cat nmapoutput.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-15 07:29 EST
Nmap scan report for 185.5.123.254
Host is up (0.055s latency).
Nmap scan report for 185.5.123.254
Host is up (0.056s latency).
Nmap done: 2048 IP addresses (2 hosts up) scanned in 985.76 seconds
```

```
┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ nmap -p80,443 --script http-methods -iL targets.txt > nmap_targets.txt
```

```
Nmap scan report for connect-us.tomtom.com (216.107.194.132)
Host is up (0.00020s latency).
rDNS record for 216.107.194.132: 216-107-194-132.static.firstlight.net

PORT    STATE    SERVICE
80/tcp  filtered http
443/tcp filtered https

Nmap scan report for mapinputtracker.tomtom.com (185.5.122.63)
Host is up (0.00028s latency).

PORT    STATE    SERVICE
80/tcp  filtered http
443/tcp filtered https

Nmap scan report for mmc-melco-prod-blue-westeurope.prod-ams.tomtom.com (20.56.251.187)
Host is up (0.00015s latency).

PORT    STATE    SERVICE
80/tcp  filtered http
443/tcp filtered https

Nmap scan report for state-reader-to-parent-26243.18292.discos.orbis.tomtom.com (20.13.86.240)
Host is up (0.013s latency).

PORT    STATE SERVICE
80/tcp  open  http
| http-methods:
|_  Supported Methods: GET HEAD POST
443/tcp open  https
```

```
┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ cat nmap_targets.txt | wc
  10335   32433  287908
```

I used httpx, a very versatile tool to valiadate a list of domains and verify whether they are alive.

```
┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ cat subdominios.txt | httpx -silent > subdominios_vivos.txt
```

This returned a list of subdomains from subdominios.txt, checked which subdomains are alive (responding to HTTP/HTTPS requests), and saved only the active subdomains in subdominios_vivos.txt.

```
┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ cat subdominios_vivos.txt | wc
     34       34      908
```

```
┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ cat subdominios_vivos.txt | unfurl --unique domains > subdominiosfinal.txt

┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ cat subdominiosfinal.txt | wc
     34       34      636
```

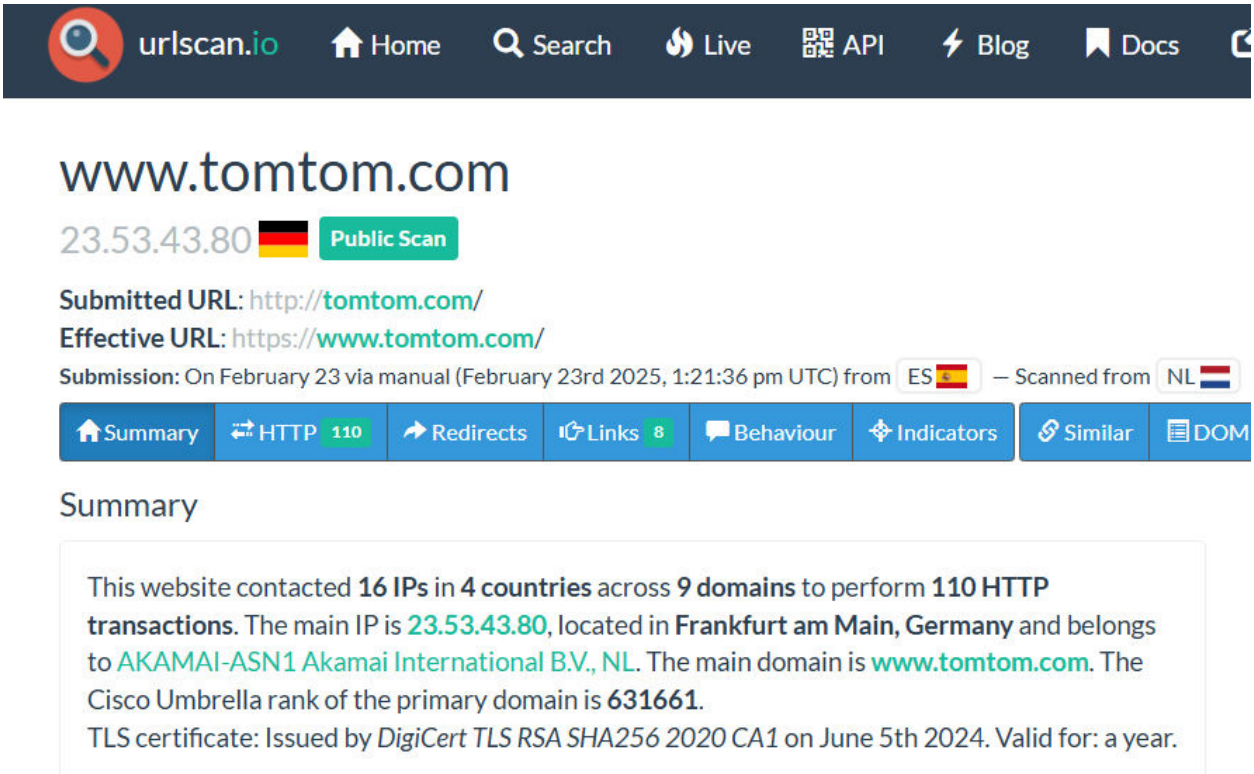
I performed a masscan to the subdominiosfinal.txt. First, I need to convert the subdomain names into IPs and for that we run the following command:

```
┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ for subdominio in $(cat subdominiosfinal.txt); do dig +short $subdominio | grep -Eo '([0-9]{1,3}.){3}[0-9]{1,3}'; done > subdominiosfinal_ips.txt

┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ cat subdominiosfinal_ips.txt | wc
     45      45     577
```

```
┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ sudo masscan -p0- -iL subdominiosfinal_ips.txt > masscan_final_ips.txt
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2025-02-23 15:48:38 GMT
Initiating SYN Stealth Scan
Scanning 15 hosts [65536 ports/host]
rate:  0.10-kpps, 15.67% done,   2:23:20 remaining, found=2
```

```
┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ cat masscan_final_ips.txt
Discovered open port 80/tcp on 18.154.22.125
Discovered open port 80/tcp on 216.198.53.1
```

Some basic, yet useful information about tomtom using urlscan.io. More information can be found.



The following command is used to start a web server that allows us to view the screenshots and results collected by GoWitness through a browser interface.

```
┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ gowitness report server http://localhost:7171/
2025/02/23 15:00:19 INFO starting web server host=127.0.0.1 port=7171
```

```
┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ gowitness scan file -f subdominiosfinal.txt
```

```
(kali㉿vbox)-[~/…/lists/tomtom.com/0211/screenshots]
$ ls
http——beat.tomtom.com-443.jpeg      http——orbisps.tomtomgroup.com-443.jpeg     https——tomtomgroup.com-443.jpeg
http——beat.tomtom.com-80.jpeg       http——orbisps.tomtomgroup.com-80.jpeg      https——tomtommaps.com-443.jpeg
http——devforum.tomtom.com-443.jpeg  https——beat.tomtom.com-443.jpeg           https——tomtom.nl-443.jpeg
http——devforum.tomtom.com-80.jpeg   https——devforum.tomtom.com-443.jpeg       https——tomtomplaces.com-443.jpeg
http——edp.tomtomgroup.com-443.jpeg  http——sd.tomtomgroup.com-443.jpeg         https——ttcode.com-443.jpeg
http——edp.tomtomgroup.com-80.jpeg   http——sd.tomtomgroup.com-80.jpeg          http——support.move.tomtom.com-443.jpeg
http——engage.tomtom.com-443.jpeg    http——security.tomtomgroup.com-443.jpeg    http——support.move.tomtom.com-80.jpeg
http——engage.tomtom.com-80.jpeg     http——security.tomtomgroup.com-80.jpeg     https——url-redirector-prod.tomtomgroup.com-443.jpeg
http——feedback.tomtomgroup.com-443.jpeg  https——edp.tomtomgroup.com-443.jpeg   https——www-preprod.tomtom.com-443.jpeg
http——feedback.tomtomgroup.com-80.jpeg   https——engage.tomtom.com-443.jpeg     https——www.tomtom.com-443.jpeg
```

The following tool used was wafwoof. This tool is used to identify Web Application Firewalls (WAFs) that are protecting a website. WAF Detection helps identify whether a website is protected by a WAF, and which WAF solution is being used (e.g., Cloudflare, ModSecurity, AWS WAF, etc.).

```
(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
$ wafw00f tomtom.com > waf_wafw00f.txt

(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
$ cat waf_wafw00f.txt | wc
     22      97    1098
```

```
(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
$ cat waf_wafw00f.txt

                    ( W00f! )
                    404 Hack Not Found
                                        405 Not Allowed
                                    403 Forbidden
                502 Bad Gateway     500 Internal Error

                ~ WAFW00F : v2.3.1 ~
    The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://tomtom.com
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[~] Number of requests: 7
```

```
(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
$ wafw00f -i subdominiosfinal.txt
```

When running this command, it returns information regarding the existence of firewall services such as these ones:

```
[*] Checking https://tomtomplaces.com
[+] The site https://tomtomplaces.com is behind Cloudfront (Amazon) WAF.
```

```
[*] Checking https://status.tomtom.com
[+] The site https://status.tomtom.com is behind BIG-IP Local Traffic Manager (F5 Networks) WAF.
```

```
[*] Checking https://itsd.tomtomgroup.com
[+] The site https://itsd.tomtomgroup.com is behind Cloudfront (Amazon) WAF.
```

Regarding other subdomain groups, they do not appear to have a firewall service, however this would require a more in-depth analysis to be able to verify it.

```
[*] Checking https://groups.tomtom.com
[+] Generic Detection results:
[-] No WAF detected by the generic detection
```

```
[*] Checking https://intouch.tomtom.com
[+] Generic Detection results:
[*] The site https://intouch.tomtom.com seems to be behind a WAF or some sort of security solution
[~] Reason: The response was different when the request wasn't made from a browser.
Normal response code is "200", while the response code to a modified request is "403"
```

The output of this process is stored in the following file: wafwoof_i.txt.

```
┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ wafw00f -i subdominiosfinal.txt > wafw00f_i.txt

┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ cat wafw00f_i.txt| wc
    144     811    6602
```

The next tool used was FFUF (Fuzz Faster U Fool), a web application fuzzing tool that is used for directory and file discovery on web servers.

```
┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ wget https://raw.githubusercontent.com/danielmiessler/SecLists/refs/heads/master/Discovery/Web-Content/common.txt
```

```
┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ ffuf -w ~/recopilacion/lists/common.txt -t 10 -mc 200,401,403 -u https://tomtom.com/FUZZ > ffuf_dir-file.txt
```

The output can be found in the following file: ffuf_dir-file.txt, however no information was found. Possible reasons could be that the wordlist (common.txt) might not contain any valid paths or directories that exist on tomtom.com or the website might be blocking directory fuzzing attempts.

```
┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ cat ffuf_dir-file.txt | wc
      0       0       0
```

The next tool I used was whatweb.

```
┌──(kali㉿kali)-[~/recopilacion/lists/tomtom.com/0211]
└─$ whatweb tomtom.com

http://tomtom.com [302 Found] Country[UNITED STATES][US], HTTPServer[Microsoft-Azure-Applicatio
n-Gateway/v2], IP[98.64.11.144], RedirectLocation[https://www.tomtom.com/], Title[302 Found]
https://www.tomtom.com/ [200 OK] Cookies[tt_languagepref], Country[UNITED STATES][US], HTML5, I
P[96.16.86.142], Open-Graph-Protocol[website], Script[application/json], Strict-Transport-Secur
ity[max-age=15724800; includeSubDomains], UncommonHeaders[x-content-type-options,release,visito
r-country], X-XSS-Protection[1]
```

From the output we can recognize the hosting infrastructure: TomTom uses Microsoft Azure for hosting, the web application is running behind an Azure Application Gateway; Regarding security measures: HSTS is enabled, which prevents man-in-the-middle attacks, X-XSS-Protection is enabled, which is basic protection against cross-site scripting, X-Content-Type-Options is set, this reduces the risk of content-type-related attacks, potential follow-up recon steps: Check for other subdomains (using subfinder, amass, or crt.sh, which I have used), probe for API endpoints (https://www.tomtom.com/api/ or JSON responses), scan for open ports (nmap -p- 2.18.188.5, done as well) and use httpx to gather further HTTP response details (done).

Whatweb was also performed for all subdomains, and I stopped it after some 20 minutes. The most useful information was stored in the following file: whatweb_subd.txt.

```
┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ whatweb -i subdominiosfinal.txt > whatweb_sub.txt
```

```
┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ cat whatweb_sub.txt | wc
     69     975   35300
```

```
┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ cat whatweb_sub.txt | head
http://move.tomtom.com [301 Moved Permanently] CloudFront, Country[UNITED STATES][US], HTTPServer[CloudFront], IP[18.154.22.125],
RedirectLocation[https://move.tomtom.com/], Title[301 Moved Permanently], UncommonHeaders[x-amz-cf-pop,x-amz-cf-id], Via-Proxy[1.1
 1f450a7791321968de9b80b08a19989e.cloudfront.net (CloudFront)]
http://www.tomtom.com [301 Moved Permanently] Akamai-Global-Host, Cookies[tt_languagepref], Country[EUROPEAN UNION][EU], HTTPServe
r[AkamaiGHost], IP[2.18.188.5], RedirectLocation[https://www.tomtom.com/], UncommonHeaders[visitor-country]
http://www.ttcode.com [302 Found] Country[UNITED STATES][US], HTTPServer[Microsoft-Azure-Application-Gateway/v2], IP[98.64.11.144]
, RedirectLocation[https://help.tomtom.com/hc/articles/360013898120/], Title[302 Found]
http://office365.tomtom.com [302 Found] Country[UNITED STATES][US], HTTPServer[Microsoft-Azure-Application-Gateway/v2], IP[98.64.1
1.144], RedirectLocation[https://portal.office.com], Title[302 Found]
http://tomtom.nl [302 Found] Country[UNITED STATES][US], HTTPServer[Microsoft-Azure-Application-Gateway/v2], IP[98.64.11.144], Red
irectLocation[https://www.tomtom.com/], Title[302 Found]
http://devforum.tomtom.com [302 Found] Country[UNITED STATES][US], HTTPServer[Microsoft-Azure-Application-Gateway/v2], IP[98.64.11
.144], RedirectLocation[https://developer.tomtom.com/knowledgebase/], Title[302 Found]
http://support.move.tomtom.com [301 Moved Permanently] CloudFront, Country[UNITED STATES][US], HTTPServer[CloudFront], IP[13.224.1
15.37], RedirectLocation[https://support.move.tomtom.com/], Title[301 Moved Permanently], UncommonHeaders[x-amz-cf-pop,x-amz-cf-id
], Via-Proxy[1.1 5aa1be24b1cf8e3c10252fabac41cc26.cloudfront.net (CloudFront)]
http://sd.tomtomgroup.com [302 Found] Country[UNITED STATES][US], HTTPServer[Microsoft-Azure-Application-Gateway/v2], IP[98.64.11.
144], RedirectLocation[https://tomtom.atlassian.net/servicedesk/customer/portals], Title[302 Found]
http://ttcode.com [302 Found] Country[UNITED STATES][US], HTTPServer[Microsoft-Azure-Application-Gateway/v2], IP[98.64.11.144], Re
directLocation[https://help.tomtom.com/hc/articles/360013898120/], Title[302 Found]
http://onboarder.tomtom.com [302 Found] Country[UNITED STATES][US], HTTPServer[Microsoft-Azure-Application-Gateway/v2], IP[98.64.1
1.144], RedirectLocation[https://www.tomtom.com], Title[302 Found]
```

By running dnsrecon -d against tomtom.com, I found that the DNSSEC is not configured, which helps prevent DNS spoofing attacks. Since it's not configured, it means TomTom's domain is not protected against certain types of DNS attacks.

```
┌──(kali㉿kali)-[~]
└─$ dnsrecon -d tomtom.com

[*] std: Performing General Enumeration against: tomtom.com...
[-] DNSSEC is not configured for tomtom.com
[*]     SOA dns1.p09.nsone.net 198.51.44.9
[*]     SOA dns1.p09.nsone.net 2620:4d:4000:6259:7:9:0:1
```

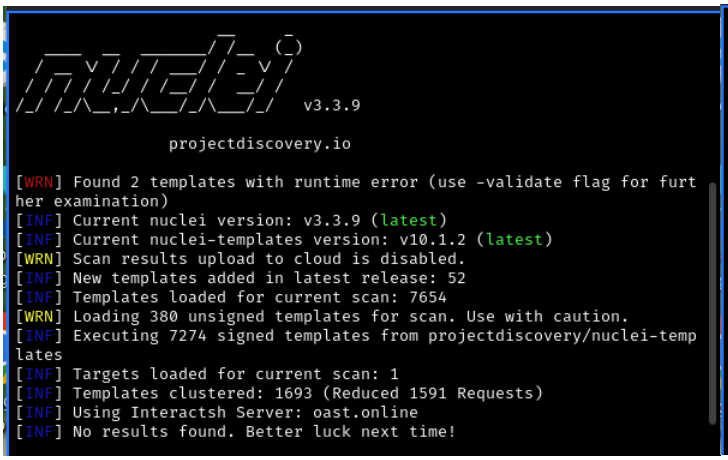
VULNERABILITY ASSESSMENT

Vulnerability Phase of Information Gathering – TomTom.com
In the vulnerability phase of information gathering, I analyze my target (in this case, TomTom.com) to identify potential security weaknesses. This phase follows initial reconnaissance, where we collect technical details like subdomains, IP addresses, server configurations, and open ports. For TomTom.com, based on previous scans, I observed the following:

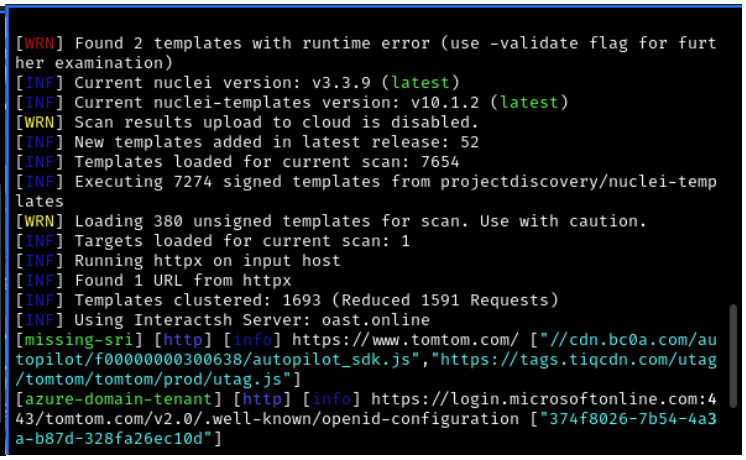
- Web Server: Microsoft Azure Application Gateway
- Security Headers: Strict-Transport-Security (HSTS), X-XSS-Protection
- Cookies: tt_languagepref
- Redirection: HTTP 302 redirect to HTTPS

Key Steps in the Vulnerability Phase include scanning for open ports & services: checking which services TomTom's servers expose (e.g., web servers, databases), analyzing web technologies & security headers, identifying outdated software, weak headers, or misconfigurations, finding subdomains & testing for live hosts, and using tools to identify and visualize active subdomains; Checking for known vulnerabilities: searching databases like CVE for security flaws in TomTom's technology stack, testing for common web exploits, and identifying weaknesses such as SQL injection, XSS, open directories, or misconfigured APIs.
This phase does not exploit vulnerabilities but focuses on identifying potential risks. It provides valuable insights for ethical hacking, penetration testing, or security assessments.

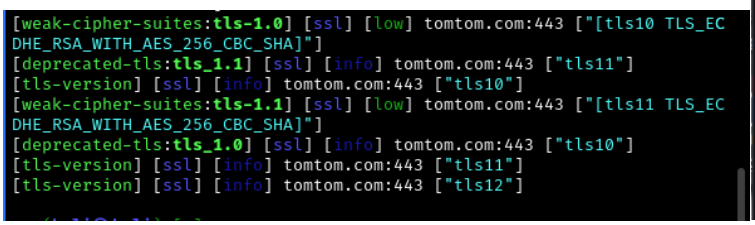
Nuclei, the first tool used, is an open-source tool used for vulnerability scanning and security testing. The results of this scan can be found in the file: nuclei_tomtom.txt.



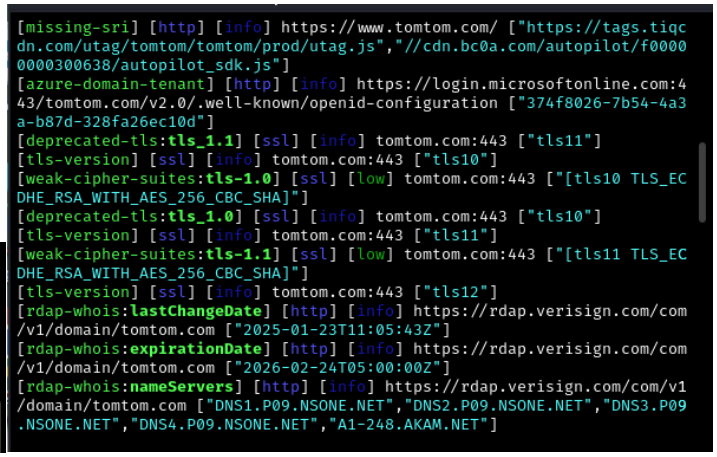
```
                     __     _
   ____  __  _______/ /__  (_)
  / __ \/ / / / ___/ / _ \/ /
 / / / / /_/ / /__/ /  __/ /
/_/ /_/\__,_/\___/_/\___/_/   v3.3.9

                projectdiscovery.io

[WRN] Found 2 templates with runtime error (use -validate flag for furt
her examination)
[INF] Current nuclei version: v3.3.9 (latest)
[INF] Current nuclei-templates version: v10.1.2 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 52
[INF] Templates loaded for current scan: 7654
[WRN] Loading 380 unsigned templates for scan. Use with caution.
[INF] Executing 7274 signed templates from projectdiscovery/nuclei-temp
lates
[INF] Targets loaded for current scan: 1
[INF] Templates clustered: 1693 (Reduced 1591 Requests)
[INF] Using Interactsh Server: oast.online
[INF] No results found. Better luck next time!
```



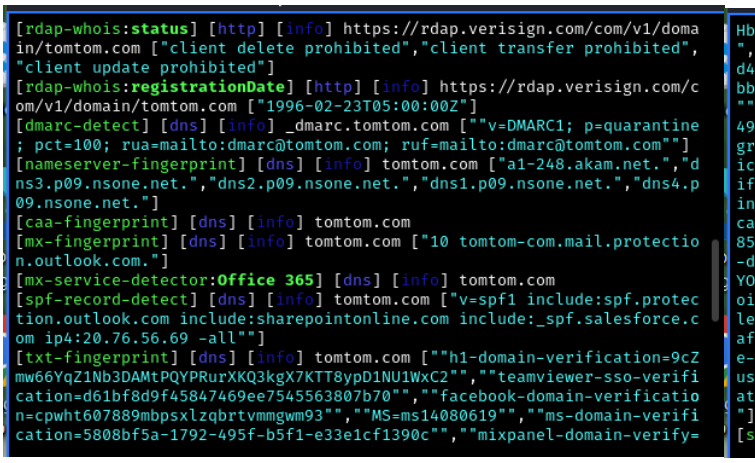
```
[WRN] Found 2 templates with runtime error (use -validate flag for furt
her examination)
[INF] Current nuclei version: v3.3.9 (latest)
[INF] Current nuclei-templates version: v10.1.2 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 52
[INF] Templates loaded for current scan: 7654
[INF] Executing 7274 signed templates from projectdiscovery/nuclei-temp
lates
[WRN] Loading 380 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 1
[INF] Running httpx on input host
[INF] Found 1 URL from httpx
[INF] Templates clustered: 1693 (Reduced 1591 Requests)
[INF] Using Interactsh Server: oast.online
[missing-sri] [http] [info] https://www.tomtom.com/ ["//cdn.bc0a.com/au
topilot/f00000000300638/autopilot_sdk.js","https://tags.tiqcdn.com/utag
/tomtom/tomtom/prod/utag.js"]
[azure-domain-tenant] [http] [info] https://login.microsoftonline.com:4
43/tomtom.com/v2.0/.well-known/openid-configuration ["374f8026-7b54-4a3
a-b87d-328fa26ec10d"]
```



```
[weak-cipher-suites:tls-1.0] [ssl] [low] tomtom.com:443 ["[tls10 TLS_EC
DHE_RSA_WITH_AES_256_CBC_SHA]"]
[deprecated-tls:tls_1.1] [ssl] [info] tomtom.com:443 ["tls11"]
[tls-version] [ssl] [info] tomtom.com:443 ["tls10"]
[weak-cipher-suites:tls-1.1] [ssl] [low] tomtom.com:443 ["[tls11 TLS_EC
DHE_RSA_WITH_AES_256_CBC_SHA]"]
[deprecated-tls:tls_1.0] [ssl] [info] tomtom.com:443 ["tls10"]
[tls-version] [ssl] [info] tomtom.com:443 ["tls11"]
[tls-version] [ssl] [info] tomtom.com:443 ["tls12"]
```



```
[missing-sri] [http] [info] https://www.tomtom.com/ ["https://tags.tiqc
dn.com/utag/tomtom/tomtom/prod/utag.js","//cdn.bc0a.com/autopilot/f0000
0000300638/autopilot_sdk.js"]
[azure-domain-tenant] [http] [info] https://login.microsoftonline.com:4
43/tomtom.com/v2.0/.well-known/openid-configuration ["374f8026-7b54-4a3
a-b87d-328fa26ec10d"]
[deprecated-tls:tls_1.1] [ssl] [info] tomtom.com:443 ["tls11"]
[tls-version] [ssl] [info] tomtom.com:443 ["tls10"]
[weak-cipher-suites:tls-1.0] [ssl] [low] tomtom.com:443 ["[tls10 TLS_EC
DHE_RSA_WITH_AES_256_CBC_SHA]"]
[deprecated-tls:tls_1.0] [ssl] [info] tomtom.com:443 ["tls10"]
[tls-version] [ssl] [info] tomtom.com:443 ["tls11"]
[weak-cipher-suites:tls-1.1] [ssl] [low] tomtom.com:443 ["[tls11 TLS_EC
DHE_RSA_WITH_AES_256_CBC_SHA]"]
[tls-version] [ssl] [info] tomtom.com:443 ["tls12"]
[rdap-whois:lastChangeDate] [http] [info] https://rdap.verisign.com/com
/v1/domain/tomtom.com ["2025-01-23T11:05:43Z"]
[rdap-whois:expirationDate] [http] [info] https://rdap.verisign.com/com
/v1/domain/tomtom.com ["2026-02-24T05:00:00Z"]
[rdap-whois:nameServers] [http] [info] https://rdap.verisign.com/com/v1
/domain/tomtom.com ["DNS1.P09.NSONE.NET","DNS2.P09.NSONE.NET","DNS3.P09
.NSONE.NET","DNS4.P09.NSONE.NET","A1-248.AKAM.NET"]
```



```
[rdap-whois:status] [http] [info] https://rdap.verisign.com/com/v1/doma
in/tomtom.com ["client delete prohibited","client transfer prohibited",
"client update prohibited"]
[rdap-whois:registrationDate] [http] [info] https://rdap.verisign.com/c
om/v1/domain/tomtom.com ["1996-02-23T05:00:00Z"]
[dmarc-detect] [dns] [info] _dmarc.tomtom.com [""v=DMARC1; p=quarantine
; pct=100; rua=mailto:dmarc@tomtom.com; ruf=mailto:dmarc@tomtom.com""]
[nameserver-fingerprint] [dns] [info] tomtom.com ["a1-248.akam.net.","d
ns3.p09.nsone.net.","dns2.p09.nsone.net.","dns1.p09.nsone.net.","dns4.p
09.nsone.net."]
[caa-fingerprint] [dns] [info] tomtom.com
[mx-fingerprint] [dns] [info] tomtom.com ["10 tomtom-com.mail.protectio
n.outlook.com."]
[mx-service-detector:Office 365] [dns] [info] tomtom.com
[spf-record-detect] [dns] [info] tomtom.com ["v=spf1 include:spf.protec
tion.outlook.com include:sharepointonline.com include:_spf.salesforce.c
om ip4:20.76.56.69 -all""]
[txt-fingerprint] [dns] [info] tomtom.com [""h1-domain-verification=9cZ
mw66YqZ1Nb3DAMtPQYPRurXKQ3kgX7KTT8ypD1NU1WxC2"","teamviewer-sso-verifi
cation=d61bf8d9f45847469ee7545563807b70"","facebook-domain-verificatio
n=cpwht607889mbpsxlzqbrtvmmgwm93"","MS=ms14080619"","ms-domain-verifi
cation=5808bf5a-1792-495f-b5f1-e33e1cf1390c"","mixpanel-domain-verify=
```

```
HbVE"","onetrust-domain-verification=829e27e3ec234967a16cbe0f3bae485c"
","pardot510681=40442bb65425b211ae9d2d6de714659b41600748d54e1e6ac7faee
d415190f48"","miro-verification=c366a88d6ef9552f4a93d9016e5eb3b8ec5d47
bb"","adobe-idp-site-verification=a0c9aec7-2cac-4280-b67d-87c4a648f73b
"","b3hqxdn8mym6085y5qjjmglycyytzvgf"","docker-verification=2158b838-
492e-404d-90c3-21764f1c446e"","S+J8Uhi6PW4nuHLLTx5XJGX8/4Uwh7QiFB1TIGF
grYkkEXHcG0IYkEU/xiZ0064EnxtaOuzKM8PMFJPTckzAOg==","google-site-verif
ication=WO42AZ7OcwAQhtl5RmaR0dlngJYc0bqbypY3bhH6XbM"","google-site-ver
ification=UzHGW9mOc94-x3sIA1aH0UDc2t8EGPIWewIT72bMVBM"","onetrust-doma
in-verification=ed9b028f470a4f418effe0bb8faf3af8"","google-site-verifi
cation=AIX2eLQtiGKMjrdTkaNIjlibc69ZhosNZEQU4XvvDPY"","RV = QuoVadis=b7
857c09-11e4-4c65-8a10-df1305b6642a"","docusign=3ce7bb6d-7e84-47a7-8d4f
-dcd7de13f634"","identrust_validate=hdIpSbx0ykv6XbCNUp2sUzubdfTombetgZ
YOY4GgqG3M"","v=spf1 include:spf.protection.outlook.com include:sharep
ointonline.com include:_spf.salesforce.com ip4:20.76.56.69 -all"","app
le-domain-verification=NAGVDc5TxR8AvHUb"","hcp-domain-verification=865
afc456cf26f92967c598d0c27a913040e4e23b8167e02f022db1a3bc929c1"","googl
e-site-verification=GzfIXCzElSCZaGP3KID04CgZ-JIxTa2KDF5kOPiuxbE"","doc
usign=4e2ef447-c398-49eb-885f-93a3c38cb230"","atlassian-domain-verific
ation=LNTzFCPe79DXpAt4NY1pKp5ZNIuZFPoQQ00EHwKjcQX1W0QLQDEDLEftCwNPoaJc"
"]
[ssl-issuer] [ssl] [info] tomtom.com:443 ["IdenTrust"]
```

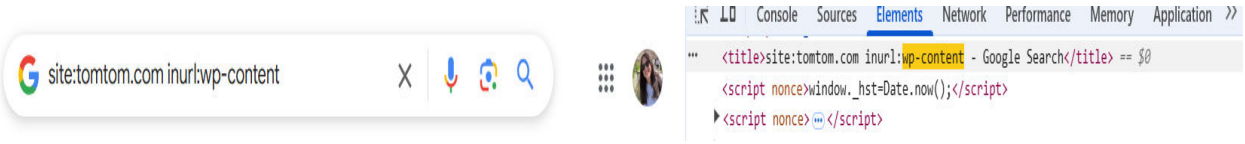
```
[ssl-issuer] [ssl] [info] tomtom.com:443 ["IdenTrust"]
[ssl-dns-names] [ssl] [info] tomtom.com:443 ["tomtom.com","tomtommaps.c
om","beat.tomtom.com","hrsd.tomtomgroup.com","orbisps.tomtomgroup.com",
"engage.tomtom.com","groups.tomtom.com","ttcode.com","sd.tomtomgroup.co
m","devforum.tomtom.com","url-redirector-prod.tomtomgroup.com","tomtom.
fi","openlr.org","tomtomplaces.com","it.tomtomgroup.com","onboarder.tom
tom.com","tomtom.nl","itsupport.tomtomgroup.com","www.ttcode.com","into
uch.tomtom.com","thebeat.tomtom.com","security.tomtomgroup.com","tomtom
group.com","edp.tomtomgroup.com","itsd.tomtomgroup.com","office365.tomt
om.com","feedback.tomtomgroup.com"]
```

```
┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ nuclei -u tomtom.com > nuclei_tomtom.txt
```


```
┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ nuclei -u tomtom.com > nuclei_tomtom.txt
```


```
┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ cat nuclei_tomtom.txt | wc
     18     108    5266
```

Web Analysis with WPScan. WPScan is a tool specifically designed for WordPress that scans for common vulnerabilities, outdated software, weak passwords, and other security risks.

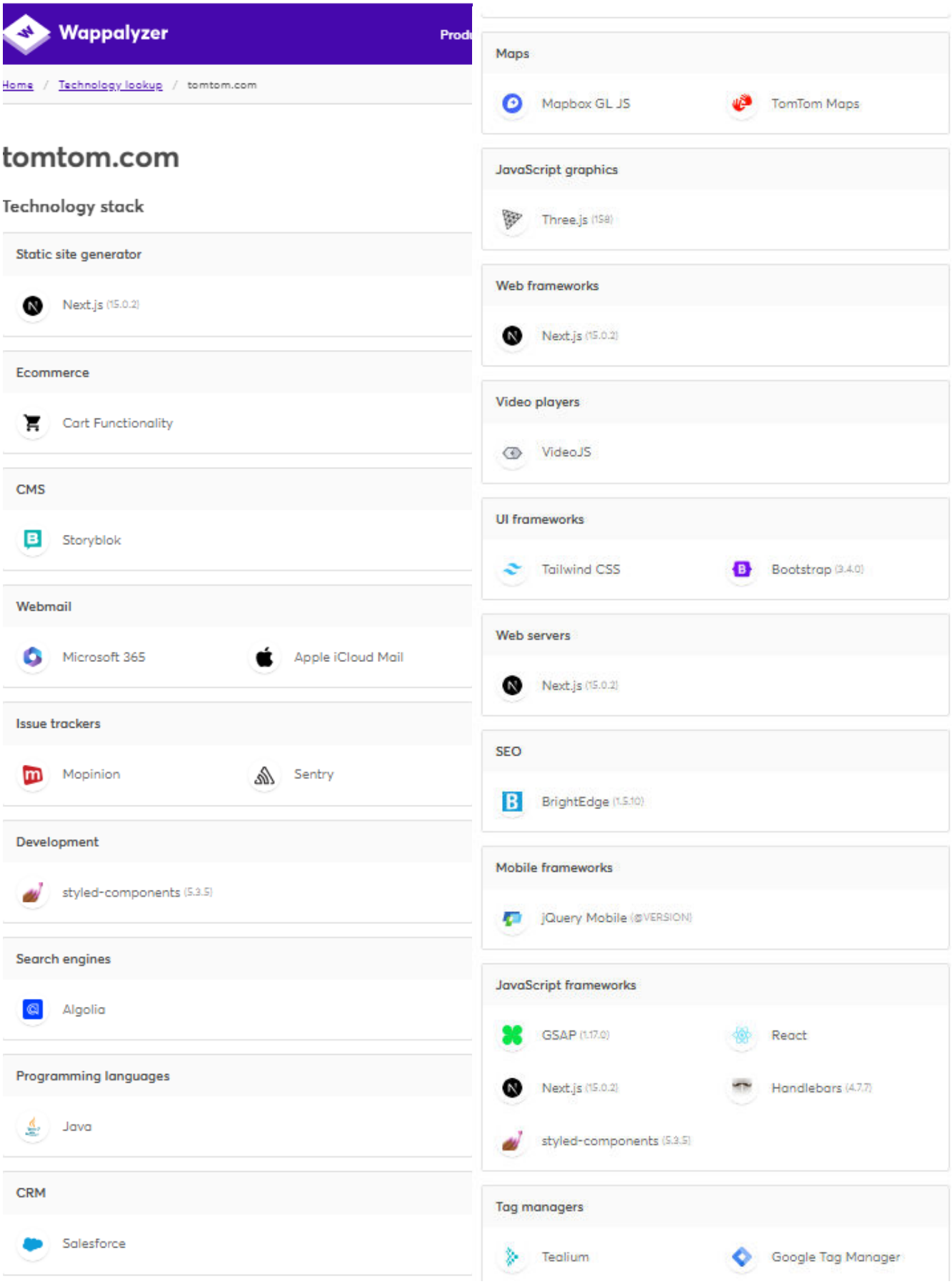



```
┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ wpscan --url https://www.tomtom.com
```

```
Scan Aborted: The remote website is up, but does not seem to be running WordPress.
```

This means that TomTom.com does not use WordPress as its CMS (Content Management System). Since WPScan only works on WordPress-based sites, it couldn't analyze TomTom.com.

Next tool: Wappalyzer. This tool analyzes technologies used by a website. Here are the key highlights.



Security

- HSTS
- hCaptcha (1)
- Akamai Web Application Protector

SSL/TLS certificate authorities

- DigiCert

Personalisation

- Demandbase (11.0.10)

Performance

- Priority Hints

Marketing automation

- HubSpot
- Salesforce Marketing Cloud Account Engagement

JavaScript libraries

- Preact
- core-js (3.29.0)
- Goober
- jQuery (3.3.1)
- MobX
- Moment.js (2.30.1)
- Modernizr (2.8.3)
- Lodash (4.17.21)

Email

- Microsoft 365

Customer data platform

- Tealium

Cookie compliance

- OneTrust

CDN

- Akamai

Analytics

- Google Analytics (GA4)
- VWO
- Contentsquare
- Demandbase (11.0.10)
- Facebook Pixel (2.9.179)
- Linkedin Insight Tag
- Mixpanel

Advertising

- Twitter Ads
- Google Ads

A/B Testing

- VWO
- Contentsquare

Miscellaneous

- Open Graph
- Webpack
- HTTP/2
- DocuSign

Detecting web technologies

```
┌──(kali㉿kali)-[~/recopilacion/lists/tomtom.com/0211]
└─$ curl -I https://tomtom.com

HTTP/1.1 302 Moved Temporarily
Server: Microsoft-Azure-Application-Gateway/v2
Date: Sat, 15 Feb 2025 15:08:35 GMT
Content-Type: text/html
Content-Length: 171
Connection: keep-alive
Location: https://www.tomtom.com/
```

Firewall or IDS detection

```
┌──(kali㉿kali)-[~/recopilacion/lists/tomtom.com/0211]
└─$ sudo nmap -sX -Pn -vv --reason -F tomtom.com

Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-15 10:10 EST
Initiating Parallel DNS resolution of 1 host. at 10:10
Completed Parallel DNS resolution of 1 host. at 10:10, 11.07s elapsed
Initiating XMAS Scan at 10:10
Scanning tomtom.com (98.64.11.144) [100 ports]
Completed XMAS Scan at 10:11, 21.32s elapsed (100 total ports)
Nmap scan report for tomtom.com (98.64.11.144)
Host is up, received user-set.
Scanned at 2025-02-15 10:10:39 EST for 21s
All 100 scanned ports on tomtom.com (98.64.11.144) are in ignored states.
Not shown: 100 open|filtered tcp ports (no-response)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 32.46 seconds
           Raw packets sent: 200 (8.000KB) | Rcvd: 0 (0B)
```

Fragmented scanning to elude detection

```
┌──(kali㉿kali)-[~/recopilacion/lists/tomtom.com/0211]
└─$ sudo nmap -f -Pn -sS -sV -O tomtom.com

Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-15 10:13 EST
Nmap scan report for tomtom.com (98.64.11.144)
Host is up (0.049s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
443/tcp open  ssl/http Microsoft Azure Application Gateway v2
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 close
d port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host

OS and Service detection performed. Please report any incorrect results at https://nmap.org/sub
mit/ .
Nmap done: 1 IP address (1 host up) scanned in 1464.52 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -Pn -O --osscan-guess tomtom.com

[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-15 10:17 EST
Nmap scan report for tomtom.com (98.64.11.144)
Host is up (0.049s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 close
d port
Device type: general purpose
Running (JUST GUESSING): OpenBSD 4.X (85%)
OS CPE: cpe:/o:openbsd:openbsd:4.0
Aggressive OS guesses: OpenBSD 4.0 (85%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.87 seconds
```

OSINT

Running theHarvester provides a wealth of publicly-available information about tomtom, such as Email addresses, Subdomains, IP addresses, Employee names, Domains & hosts, Social media accounts, and Pastes and data leaks. The results can be found in the file: theHarvesterfinds.txt.

```
┌──(kali㉿kali)-[~]
└─$ theHarvester -d tomtom.com -b bing

Read proxies.yaml from /etc/theHarvester/proxies.yaml
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.6.0                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************
```

```
┌──(kali㉿kali)-[~]
└─$ theHarvester -d tomtom.com -b all
```

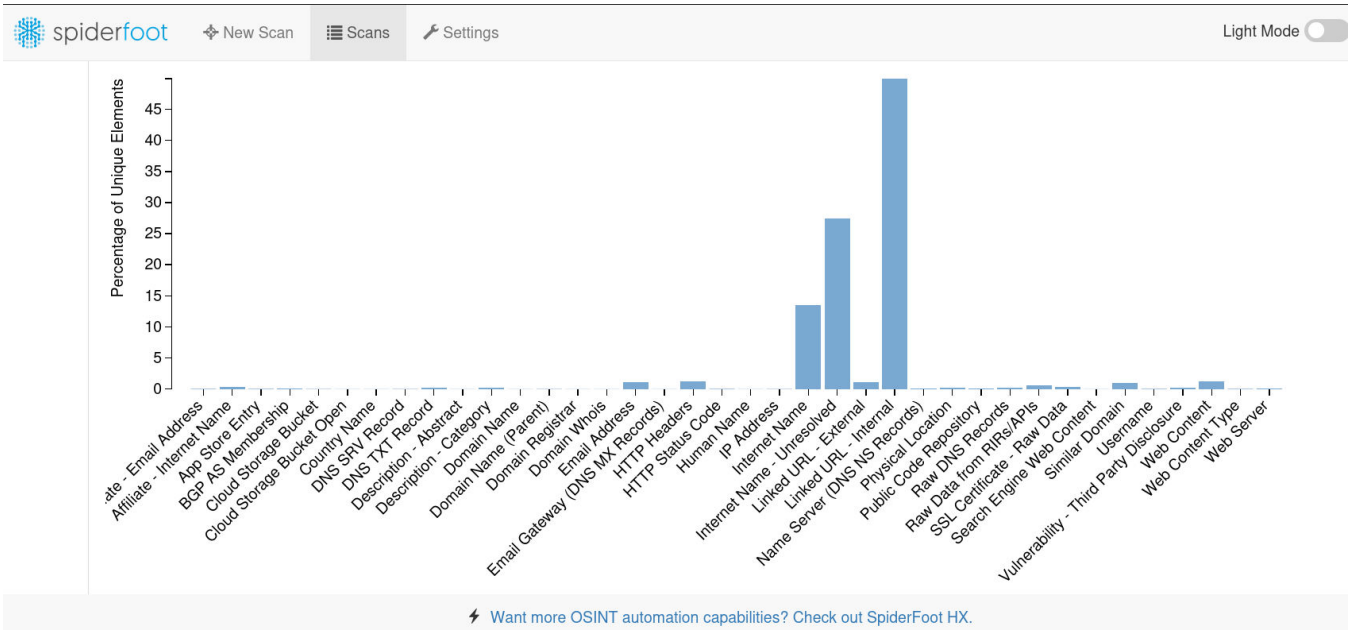
```
┌──(kali㉿kali)-[~]
└─$ theHarvester -d tomtom.com -b all > theHarvesterfinds.txt
```

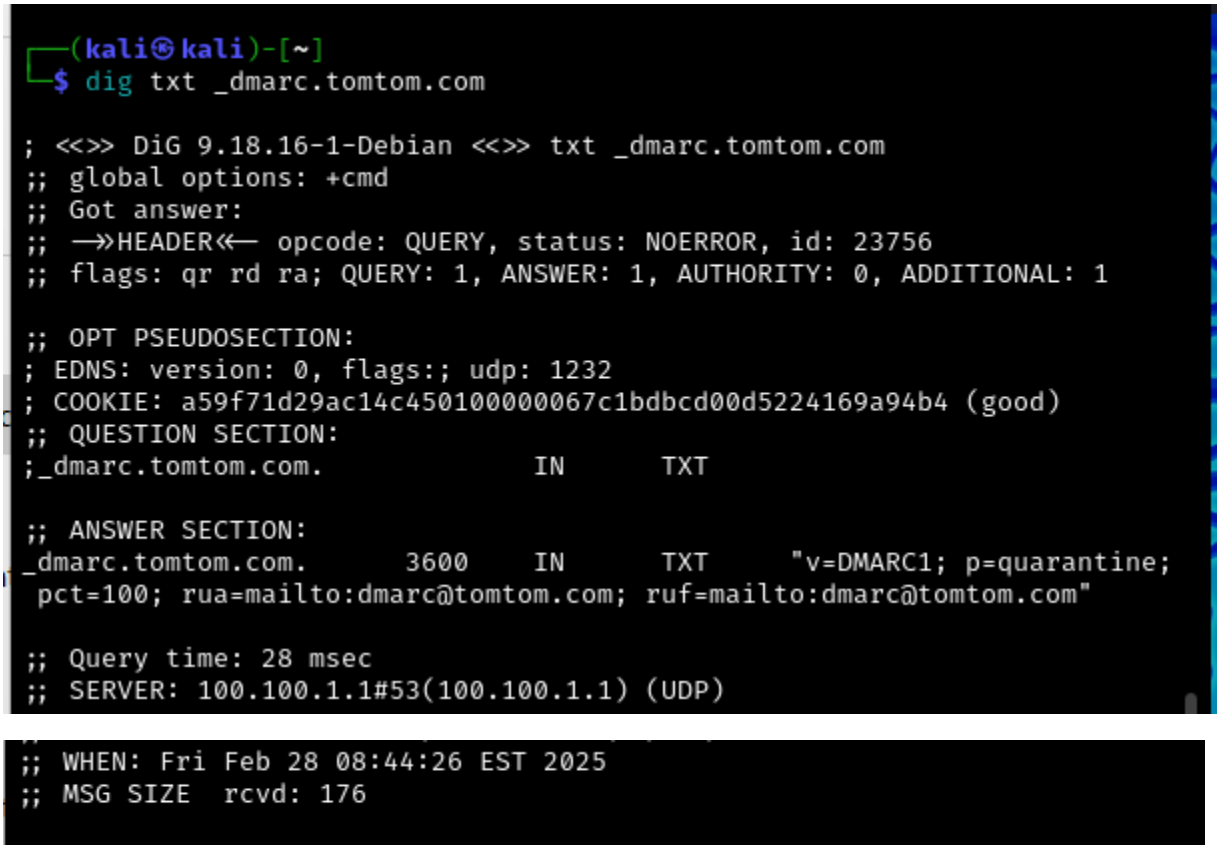
```
┌──(kali㉿kali)-[~]
└─$ cat theHarvesterfinds.txt | wc
   7776    8218  334947
```

```
┌──(kali㉿kali)-[~]
└─$ cat theHarvesterfinds.txt | grep -i "password"

reset-password.mep.tomtom.com
reset-password.mep.tomtom.com:51.145.188.111

┌──(kali㉿kali)-[~]
└─$ cat theHarvesterfinds.txt | grep -E -o "[A-Za-z0-9._%+-]+@[A-Za-z0-9.-]+\.[A-Za-z]{2,}"

cmartorella@edge-security.com
enterpriseitbiztalk@groups.tomtom.com
```

```
┌──(kali㉿kali)-[~]
└─$ cat theHarvesterfinds.txt | grep "tomtom" | sort -u

10099.discos.orbis.tomtom.com
11066.discos.orbis.tomtom.com
12529.discos.orbis.tomtom.com
12598.discos.orbis.tomtom.com
12928.discos.orbis.tomtom.com
13436.discos.orbis.tomtom.com
14706.orbis.tomtom.com
14871.orbis.tomtom.com
14878.discos.orbis.tomtom.com
16971.discos.orbis.tomtom.com
17198.discos.orbis.tomtom.com
17696.koc.discos.orbis.tomtom.com
18292.discos.orbis.tomtom.com
18292.discos-staging.orbis.tomtom.com
18292.koc.discos.orbis.tomtom.com
18651.discos.orbis.tomtom.com
```

Spiderfoot was used to check tomtom.com. The full results are in the .xlsx file.

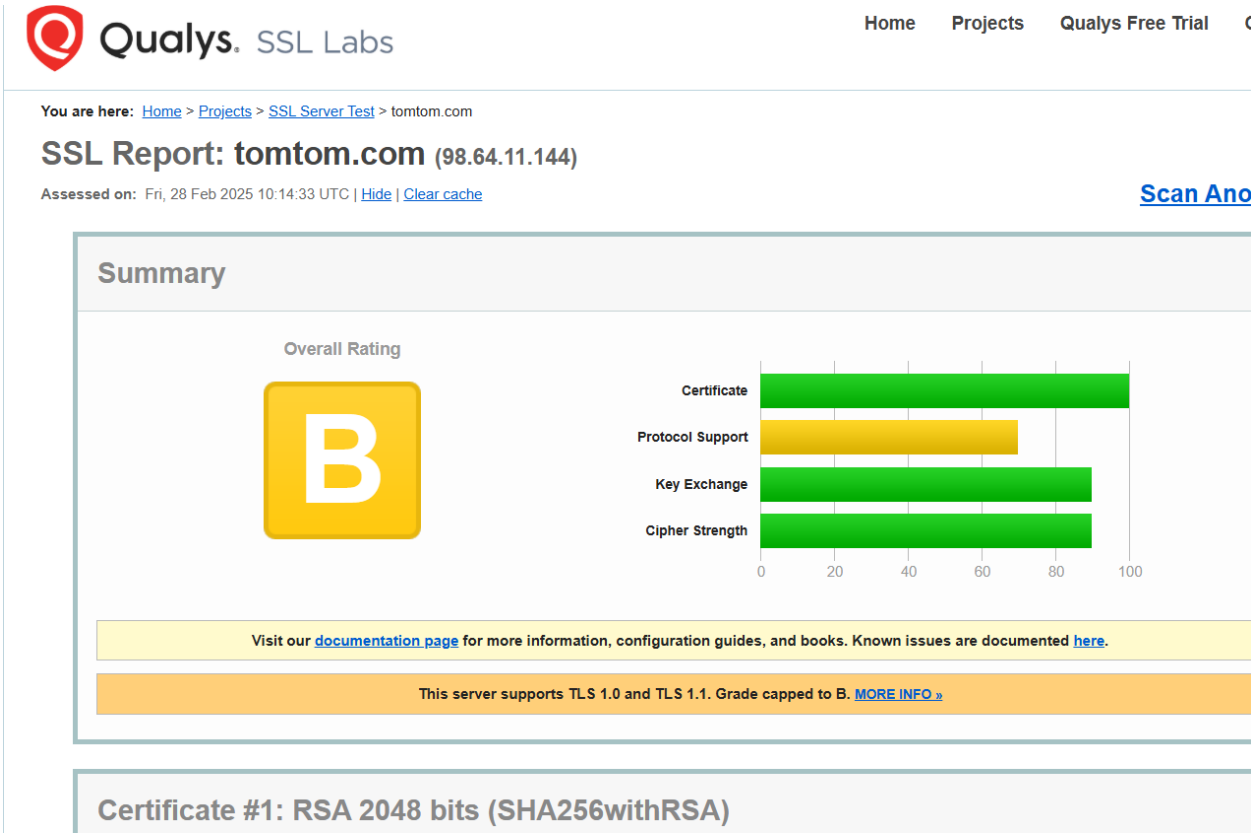




This means TomTom has DMARC configured with the following parameters:

- v=DMARC1 → Protocol Version
- p=quarantine → DMARC policies indicate that the emails where authentication fails, they must be marked as spam or quaratined.
- pct=100 → This policy is applied to all mail.
- rua=mailto:dmarc@tomtom.com → Email address where TomTom receives all added reports from DMARC (statistics).
- ruf=mailto:dmarc@tomtom.com → Email address where TomTom receives all forensic emails (detailed emails about email authentication failures).

I ran tomtom.com on Qualys SSL Labs. This tool provides detailed security analysis of SSL/TLS configurations for websites. It performs a thorough scan of the website's SSL/TLS setup and generates a report, helping identify any issues or vulnerabilities and providing recommendations to improve security.



I used testssl.sh to check the security of SSL/TLS (Secure Sockets Layer/Transport Layer Security) configurations on TomTom's web server. It helps identify vulnerabilities and provides an in-depth analysis of how well the server is configured to protect communications over the internet. When you run a command using testssl.sh, it performs a series of tests to evaluate the security of the SSL/TLS configuration of the specified server or domain.

The results of this process were saved in a file named testssl_tomtom.txt.

Mails Servers Authentication (SPF, DKIM, and DMARC)

These three mechanisms—SPF, DKIM, and DMARC—work together to improve email security by authenticating the origin and integrity of messages, preventing spoofing, and helping domain owners monitor the effectiveness of their email authentication.

https://dmarcian.com/domain-checker/?domain=tomtom.com results:

dmarcian.com/domain-checker/?domain=tomtom.com

DMARC

Your domain has a valid DMARC record and it is set to p=quarantine. To fully take advantage of DMARC, the policy should be set to p=reject.

— Details

```
v=DMARC1; p=quarantine; pct=100; rua=mailto:dmarc@tomtom.com; ruf=mailto:dmarc@tomtom.com
```

SPF

Great job! You have a valid SPF record, which specifies a hard fail (-all).

— Details

```
v=spf1 include:spf.protection.outlook.com include:sharepointonline.com include:_spf.salesforce.com ip4:20.76.56.69 -all
```

DKIM

We found at least one DKIM valid record. It's likely that you have others as each email sending source should have its own DKIM keys. DMARC visibility can help you discover each of your DKIM keys and much more.

— Details

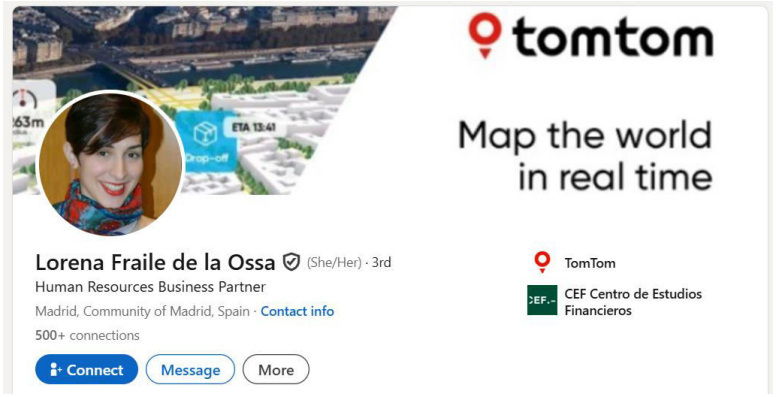
```
v=DKIM1; k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDOH0YkmjJnJdNDgfyIZwoOppvs08+lX8UC1mERk+kyk1hN/0d+zwx22eUVevNYvgk40n67g0uvPK2Si
giRPV2cfgzgtXU+5tMWfdzHemYZztHtjgGROZvax1MNUdMLLNsy9HisJmeECUzq5HqFnwQZmaeIxaG5cO6Hb+NHIgs/bQIDAQAB;
```

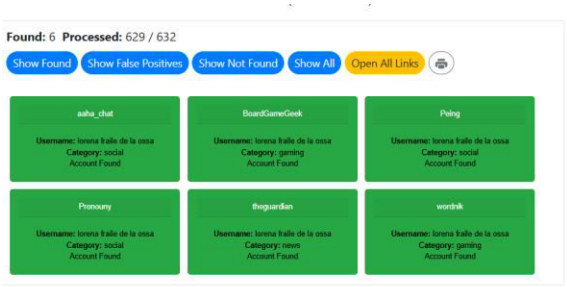
I ran Subzy to detect subdomain takeover vulnerabilities.

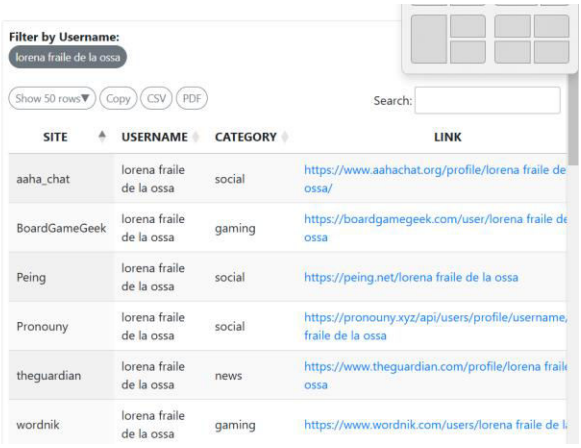
```
┌──(kali㉿vbox)-[~/spoofcheck]
└─$ sudo ln -s $HOME/go/bin/subzy /usr/bin/subzy
```

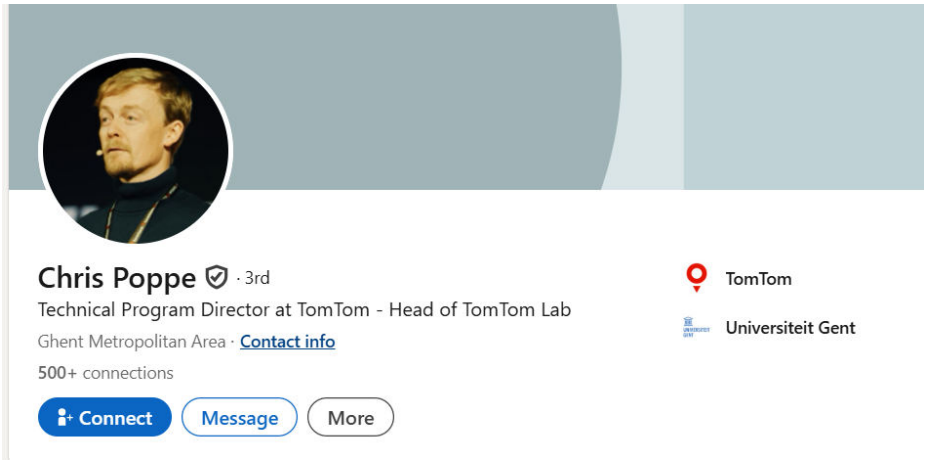
```
┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ subzy run --targets subdominios_vivos.txt > subzy_subd_vivos.txt

┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ cat subdominios_vivos.txt | wc
     34      34     908

┌──(kali㉿vbox)-[~/recopilacion/lists/tomtom.com/0211]
└─$ cat subdominios_vivos.txt | head
https://www.tomtom.com
https://onboarder.tomtom.com
https://hrsd.tomtomgroup.com
https://www.ttcode.com
https://devforum.tomtom.com
https://tomtommaps.com
https://beat.tomtom.com
https://security.tomtomgroup.com
https://office365.tomtom.com
https://tomtomplaces.com
```

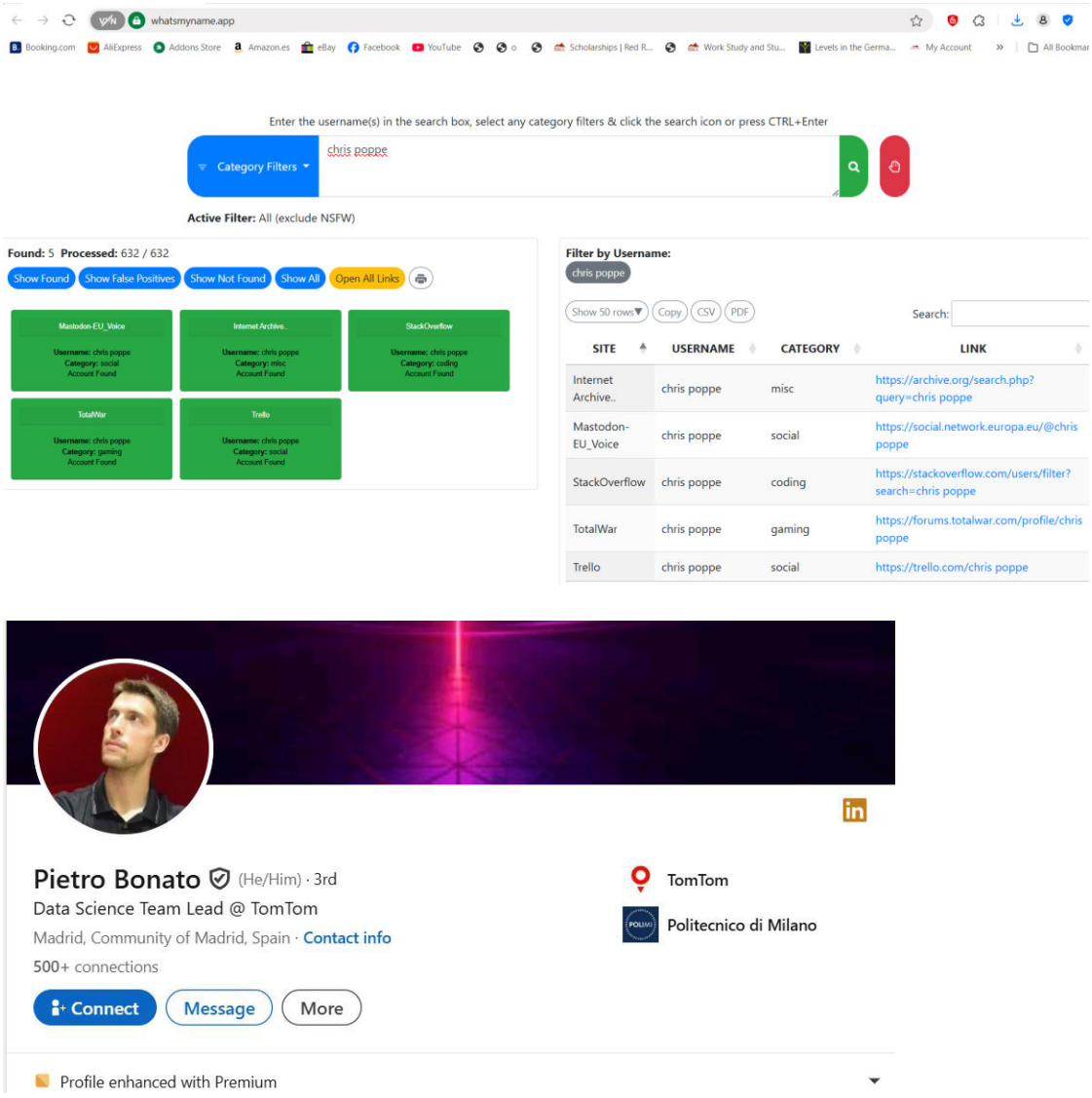
Whatsmyname.app didn't come up with very reliable results. One example is that I searched for my name, and all the results were false positives. I have no relation whatsoever with any of those websites. I have included the names of some employees holding a relevant position at tomtom.



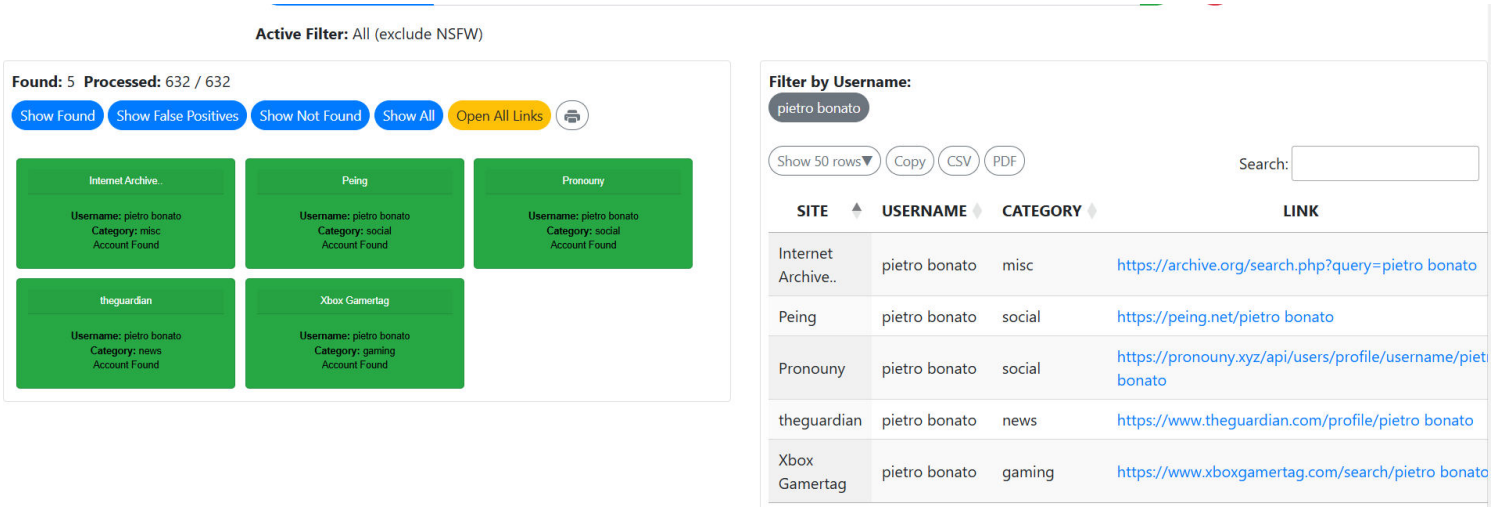







whatsmyname.app
Enter the username(s) in the search box, select any category filters & click the search icon or press CTRL+Enter
Category Filters
chris poppe
Active Filter: All (exclude NSFW)
Found: 5 Processed: 632 / 632
Show Found
Show False Positives
Show Not Found
Show All
Open All Links
Mastodon-EU_Voice
Internet Archive..
StackOverflow
TotalWar
Trello
Filter by Username:
chris poppe
Show 50 rows
Copy
CSV
PDF
Search:
SITE
USERNAME
CATEGORY
LINK
Internet Archive.. chris poppe misc https://archive.org/search.php?query=chris poppe
Mastodon-EU_Voice chris poppe social https://social.network.europa.eu/@chris poppe
StackOverflow chris poppe coding https://stackoverflow.com/users/filter?search=chris poppe
TotalWar chris poppe gaming https://forums.totalwar.com/profile/chris poppe
Trello chris poppe social https://trello.com/chris poppe

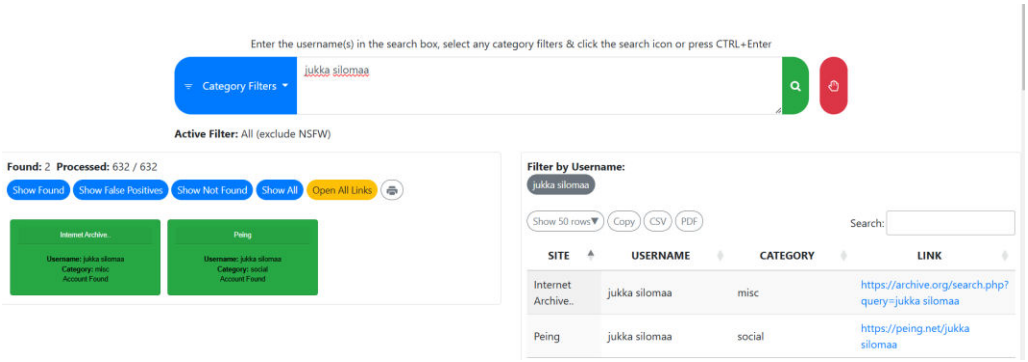
Pietro Bonato (He/Him) · 3rd
Data Science Team Lead @ TomTom
Madrid, Community of Madrid, Spain · Contact info
500+ connections
Connect
Message
More
TomTom
Politecnico di Milano
Profile enhanced with Premium

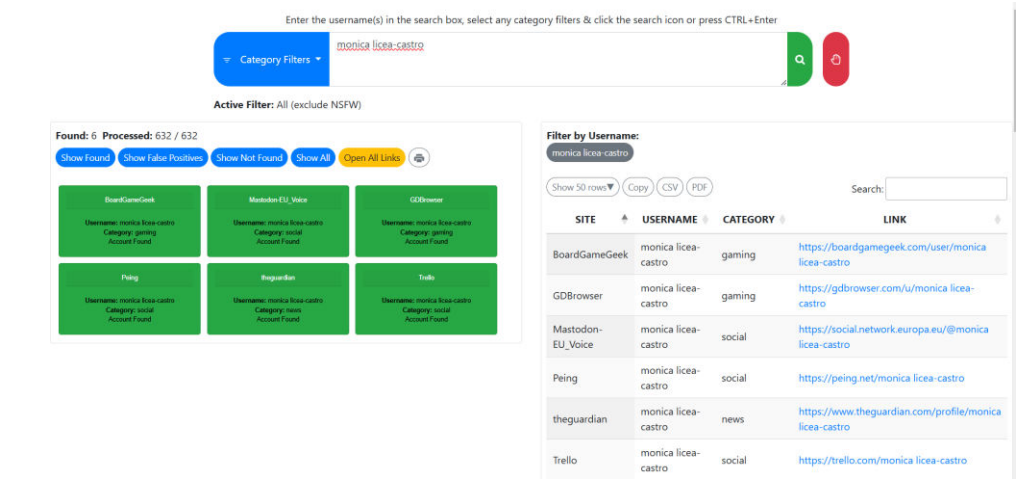

Active Filter: All (exclude NSFW)
Found: 5 Processed: 632 / 632
Show Found
Show False Positives
Show Not Found
Show All
Open All Links
Internet Archive..
Peing
Pronouny
theguardian
Xbox Gamertag
Filter by Username:
pietro bonato
Show 50 rows
Copy
CSV
PDF
Search:
SITE
USERNAME
CATEGORY
LINK
Internet Archive.. pietro bonato misc https://archive.org/search.php?query=pietro bonato
Peing pietro bonato social https://peing.net/pietro bonato
Pronouny pietro bonato social https://pronouny.xyz/api/users/profile/username/piet bonato
theguardian pietro bonato news https://www.theguardian.com/profile/pietro bonato
Xbox Gamertag pietro bonato gaming https://www.xboxgamertag.com/search/pietro bonato

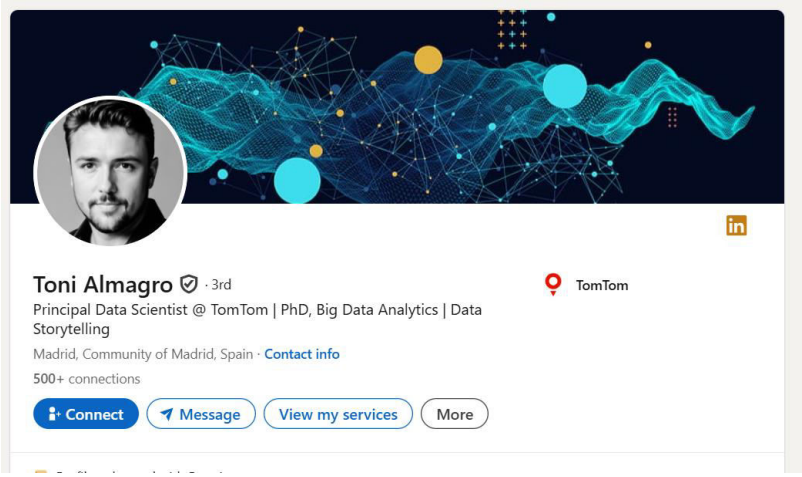
Jukka Silomaa · 3rd
Governance, Risk & Compliance | Strategy | Cybersecurity | Leadership | CISO
Amsterdam, North Holland, Netherlands · Contact info
3,721 followers · 500+ connections

TomTom
Harvard University

+ Follow | Message | More







Toni Almagro · 3rd
Principal Data Scientist @ TomTom | PhD, Big Data Analytics | Data Storytelling
Madrid, Community of Madrid, Spain · Contact info
500+ connections

TomTom

Connect | Message | View my services | More

Files

The following files can be found in the folder "recopilación de información" in the GitHub repository:

Text Document

- allports
- alterx
- cero
- ctfr
- ctfr_limpio
- dnsrecon3
- gau
- gauoutput
- katana
- katanaoutput
- masscan_final_ips
- nmap_targets
- nmapoutput
- nslookup
- nuclei_tomtom
- resolvers
- subdominios
- subdominios_vivos
- subdominiosfinal
- subdominiosfinal_ips
- subdominiosvivos
- subfinder (1)
- subfinder
- targets
- testssl
- theHarvesterfinds
- waf_wafw00f
- wafw00f_i
- whatweb_sub
- whois
- whoistomtom

PNG File

- tomtom

Microsoft Excel Worksheet

- 1._ExcelTables_WEBSITE_Q3_2015(1)
- 1._ExcelTables_WEBSITE_Q3_2015
- Excel Tables Website - Q1 2024
- Excel Tables Website - Q3 2020(1)
- Excel Tables Website - Q3 2020
- Excel_Tables_Website_Q1_2019(1)
- Excel_Tables_Website_Q1_2019
- ExcelTables_WEBSITE
- Financial overview(1)
- Financial overview
- Practice_Edits_B_YOURNAME (1)
- Practice_Edits_B_YOURNAME (2)
- Practice_Edits_B_YOURNAME(1)
- Practice_Edits_B_YOURNAME
- TomTomExcelTables_WEBSITE_Q4_2014
- tomtom-SpiderFoot

Microsoft Excel Comma Separated Values File	Microsoft Edge PDF Document	Microsoft Edge MHT Document
Reverse-WHOIS-DRS-report-tomtom.com	crt.sh _ tomtom.com	Technologies used on tomtom.com - Wappalyzer
	Maltego-tomotm	
	tomtom.com - Reverse Whois Lookup - ViewDNS.info	
	tomtom.com DNS Records - ViewDNS.info	

The information gathering phase on TomTom.com was carried out using a structured approach involving vertical footprinting, fingerprinting, vulnerability assessment, and OSINT techniques. The results provided a detailed understanding of the organization's online presence, technologies in use, and potential security concerns.

Vertical Footprinting

This phase focused on identifying TomTom's external infrastructure using various techniques:TLS Probing (cero) provided details on supported cryptographic protocols, confirming that TLS encryption is in place, Web Scraping (katana) extracted useful URLs and linked resources from the site, Certificate Transparency Logs (ctfr) uncovered historical and currently active subdomains, Archived Web Content & Caching (gau) retrieved older versions of web pages, providing insights into past configurations and exposed endpoints, and Subdomain Permutations (alterx + dnsx) helped expand the list of potential subdomains for further testing.

◈ **Key Insight**: TomTom has a well-structured cloud-based infrastructure with multiple subdomains, some of which may host third-party services.

Fingerprinting

The goal of this phase was to identify online assets, services, and security mechanisms. Subdomain Status Check (httpx) filtered out live subdomains from the initial list, Port Scanning & Service Detection (masscan / nmap) revealed open ports and running services, confirming the use of Azure cloud services, Technology Identification (gowitness / Wappalyzer / whatweb) showed that TomTom.com is a custom-built application, not based on a CMS like WordPress, and uses technologies such as Microsoft Azure and various security headers, Web Application Firewall (WAF) Detection (wafwoof) confirmed the presence of security protections, making direct attacks harder, Content Discovery / Fuzzing (ffuf) attempted to find hidden directories or sensitive files, though no critical exposures were found.

◈ **Key Insight**: TomTom uses a custom-built application with strong security measures, making traditional CMS-based exploits ineffective.

Vulnerability Analysis

This phase aimed to detect potential weaknesses in TomTom's security posture. Standard Vulnerability Scanning (Greenbone & Nuclei) checked for known vulnerabilities but found no immediate high-risk issues, Web Application Scanning (wpscan) confirmed that TomTom.com does not run on WordPress, leading to an aborted scan, SSL/TLS Security Analysis assessed certificate strength and encryption protocols, verifying that strong encryption is in use, Email Security Assessment (DMARC/DKIM/SPF) analyzed TomTom's email security policies, reducing the risk of email spoofing attacks, Subdomain Takeover Detection (subzy) ensured that unused or misconfigured subdomains were not vulnerable to being hijacked.

◈ Key Insight: TomTom.com has good security practices in place, with no immediately exploitable vulnerabilities found.

OSINT (Open-Source Intelligence)

Gathering publicly available information about TomTom and its employees provided additional insights: Email & User Enumeration (Maltego / Spiderfoot) did not reveal any publicly exposed credentials, Metadata Analysis (exiftool + search engines) did not find leaked sensitive documents or internal information, Employee Research (LinkedIn & social media analysis) identified potential employees of interest based on job roles, but no direct security concerns.

◈ **Key Insight**: There is no publicly available sensitive information that could be immediately leveraged in an attack.

Key Takeaways:

Strong Security Posture – TomTom employs cloud-based security, WAF protection, and TLS encryption, reducing the attack surface.

No Immediate Critical Vulnerabilities – The scans did not reveal serious security flaws, though further testing could focus on misconfigured services or third-party integrations.

Limited Publicly Available Information – OSINT efforts did not uncover critical leaks, meaning TomTom maintains good control over its public exposure.

WRITE apto HERE ⟶ _____