

DNS Reconnaissance Report: infosys.com

Date of Analysis: August 30, 2025

Author: Ishaan Malhotra

Target Domain: infosys.com

1. Executive Summary

This report details the findings from a passive DNS reconnaissance performed on the domain `infosys.com`. The objective was to gather publicly available information about the domain's infrastructure, including IP addresses, mail servers, name servers, and associated subdomains. The analysis utilized several standard command-line tools: `whois`, `dnsenum`, `dnsrecon`, `dnsmap`, `dig`, and `nslookup`.

Key findings indicate that `infosys.com` uses third-party services for its DNS (CSC), content delivery (Akamai), and email security (Trend Micro). A number of public-facing subdomains were discovered, pointing to various services including blogs, identity management (Salesforce), and IT portals. A crucial security check, the DNS Zone Transfer, was attempted and was successfully refused by the name servers, indicating a positive security posture in that regard.

2. Methodology

The following tools were used to gather information for this report:

- **whois:** To retrieve domain registration details.
- **dnsenum:** For general DNS enumeration, including A, NS, and MX records, and zone transfer attempts.
- **dnsrecon:** For brute-forcing subdomains using a dictionary list.
- **dnsmap:** For additional subdomain discovery.
- **dig:** For specific DNS record queries (MX).
- **nslookup:** For standard DNS queries and mail server lookups.

3. Detailed Findings

3.1. WHOIS Information

The `whois` lookup provided the following registration details for the domain:

- **Domain Name:** INFOSYS.COM
- **Registrar:** MarkMonitor Inc.
- **Creation Date:** 1996-07-17
- **Name Servers:**
 - udsn1.cscdns.net
 - udsn2.cscdns.net
- **Domain Status:** The domain is protected with `clientTransferProhibited`, `clientUpdateProhibited`, and `clientDeleteProhibited` statuses, preventing unauthorized transfers, updates, or deletions.

Evidence: whois command output.

```
L$ whois infosys.com
Domain Name: INFOSYS.COM
Registry Domain ID: 3015991_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: http://cscdbs.com
Updated Date: 2025-08-01T07:47:53Z
Creation Date: 1992-07-17T04:00:00Z
Registry Expiry Date: 2025-10-13T14:52:28Z
Registrar: CSC Corporate Domains, Inc.
Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: 8887802723
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
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: UDNS1.CSCDNS.NET
Name Server: UDNS2.CSCDNS.UK
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-08-30T14:13:35Z <<<
```

3.2. Core DNS Records

- A Record (Host Address):** The primary domain `infosys.com` resolves to `35.71.178.178`.
- NS Records (Name Servers):** The authoritative name servers are `udsn1.cscdns.net` and `udsn2.cscdns.uk`.
- MX Records (Mail Exchange):** The domain's email is handled by Trend Micro's email security service via `infosyslimited.in.tmes.trendmicro.eu`.

Evidence: dnsenum, dig, whois, and nslookup command outputs confirming A, NS, and MX records.

Mail (MX) Servers:					
45	infosyslimited.in.tmes.trendmicro.eu.	5	IN	A	18.185.115.1
47	infosyslimited.in.tmes.trendmicro.eu.	5	IN	A	18.185.115.1
46	infosyslimited.in.tmes.trendmicro.eu.	5	IN	A	18.185.115.1

```
—$ nslookup infosys.com 192.168.80.2
Server:      192.168.80.2
Address:     192.168.80.2#53

Non-authoritative answer:
Name:   infosys.com
Address: 35.71.178.178
```

```
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdatePr
obhibited
Name Server: UDNS1.CSCDNS.NET
Name Server: UDNS2.CSCDNS.UK
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wi
cf/
>>> Last update of whois database: 2025-08-30T14:13:35Z <<<
```

3.3. Subdomain Enumeration

The brute-force scans from dnsenum, dnsrecon, and dnsmap revealed several active subdomains:

Subdomain	Resolves To (IP Address or CNAME)	Notes
www.infosys.com	23.201.129.123 / 23.216.157.119	Akamai CDN
autodiscover.infosys.com	CNAME to infycorp.akadns.net / 122.98.14.179	Microsoft Exchange service discovery
blogs.infosys.com	13.107.246.40 / 104.108.153.144	Blog hosting
connect.infosys.com	13.107.246.68	Connection/portal service
it.infosys.com	151.101.138.133, 151.101.194.133, etc.	IT-related services
id.infosys.com	CNAME to id.infosys.com.cs20.force.com	Identity service, likely using Salesforce
adfs.infosys.com	CNAME to Akamai (e4029.dsca.akamaiedge.net)	Active Directory Federation Services
abns.infosys.com	CNAME to Akamai (e955.dsca.akamaiedge.net)	Purpose unclear

Evidence: Output from various subdomain discovery tools.

```
$ dnsrecon -d infosys.com -D /usr/share/wordlists/dnsmap.txt -t brt
[*] Using the dictionary file: /usr/share/wordlists/dnsmap.txt (provided by user)
[*] brt: Performing host and subdomain brute force against infosys.com ...
[+] CNAME abm.infosys.com abm.infosys.com.edgekey.net
[+] CNAME abm.infosys.com.edgekey.net e8955.dsca.akamaiedge.net
[+] A e8955.dsca.akamaiedge.net 23.219.57.146
[+] CNAME abm.infosys.com abm.infosys.com.edgekey.net
[+] CNAME abm.infosys.com.edgekey.net e8955.dsca.akamaiedge.net
[+] AAAA e8955.dsca.akamaiedge.net 2600:1417:55:197::22fb
[+] AAAA e8955.dsca.akamaiedge.net 2600:1417:55:18f::22fb
[+] CNAME isf.infosys.com isf-cncvgydrancfcta3.z01.azurefd.net
[+] CNAME isf-cncvgydrancfcta3.z01.azurefd.net star-azurefd-prod.trafficmanager.net
[+] CNAME star-azurefd-prod.trafficmanager.net shed.dual-low.s-part-0020.t-0009.t-msedge.net
[+] CNAME shed.dual-low.s-part-0020.t-0009.t-msedge.net s-part-0020.t-0009.t-msedge.net
[+] A s-part-0020.t-0009.t-msedge.net 13.107.246.48
[+] CNAME isf.infosys.com isf-cncvgydrancfcta3.z01.azurefd.net
[+] CNAME isf-cncvgydrancfcta3.z01.azurefd.net star-azurefd-prod.traffic
```

Brute forcing with /usr/share/dnseenum/dns.txt:

	5	IN	CNAME	(
autodiscover.infosys.com.	5	IN	CNAME	122.98.
autodiscover.infosys.com.infycorp.akadns.net.	5	IN	A	
14.179				
www.infosys.com.	5	IN	CNAME	www.infosys.
com.edgekey.net.				
www.infosys.com.edgekey.net.	5	IN	CNAME	e709.b.akama
iedge.net.				
e709.b.akamaiedge.net.	5	IN	A	23.216.157.1
19				

```
└$ dnsmap infosys.com
dnsmap 0.36 - DNS Network Mapper

[+] searching (sub)domains for infosys.com using built-in wordlist
[+] using maximum random delay of 10 millisecond(s) between requests

blogs.infosys.com
IPv6 address #1: 2600:1417:55:197::22fb
IPv6 address #2: 2600:1417:55:18f::22fb

blogs.infosys.com
IP address #1: 104.108.153.144

connect.infosys.com
IPv6 address #1: 2620:1ec:bdf::68

connect.infosys.com
IP address #1: 13.107.246.68

tl.infosys.com
IP address #1: 151.101.130.133
IP address #2: 151.101.194.133
IP address #3: 151.101.66.133
IP address #4: 151.101.2.133

www.infosys.com
IP address #1: 23.201.129.123
```

3.4. IP Blocks and Netranges

The `dnsenum` tool identified the following network ranges associated with the domain:

- 35.71.178.0/24
- 35.71.178.178/32

Evidence: `dnsenum` output showing identified netranges and IP blocks.

The screenshot shows the command-line output of the `dnsenum` tool for the domain `infosys.com`. It displays two sections: "netranges" and "ip blocks".

```
infosys.com class C netranges:  
-----  
35.71.178.0/24  
  
infosys.com ip blocks:  
-----  
35.71.178.178/32
```

4. Security Observations

- **Positive Security Control:** Attempts to perform a DNS Zone Transfer (AXFR) were **REFUSED** by both name servers (`uds1.cscdns.net` and `uds2.cscdns.uk`). This is a critical security measure that prevents an attacker from easily listing all DNS records for the domain.
- **Attack Surface:** The identified subdomains expose a wide range of services, including Microsoft Exchange, Active Directory, Salesforce, and various web portals. Each of these represents a potential vector for attack and should be independently secured and monitored.
- **Third-Party Reliance:** The infrastructure relies heavily on third-party cloud and security providers (Akamai, Trend Micro, Salesforce). The security of `infosys.com` is therefore partially dependent on the security of these vendor

5. Conclusion

The reconnaissance of `infosys.com` reveals a mature and distributed network architecture typical of a large enterprise. Standard DNS records are properly configured, and basic DNS security, such as disabling zone transfers, is correctly implemented. The information gathered provides a clear map of the publicly accessible digital footprint of the organization, which is the foundational first step in any security.

