

# Passive Reconnaissance Report: infosys.com

**Date of Assessment:** September 2, 2025

**Author:** Ishaan Malhotra

**Classification:** Confidential

## 1. Executive Summary

This report outlines the findings of a passive reconnaissance assessment conducted on the domain `infosys.com`. The objective was to gather publicly available information to understand the organization's external attack surface without directly interacting with its systems.

The investigation successfully identified a significant amount of information, including hundreds of subdomains, multiple IP addresses and network blocks, employee email addresses, and server port/service information. Furthermore, Google dorking techniques revealed potentially sensitive documents and exposed login panels.

The findings, supported by the evidence in the appendix, indicate a large and complex digital footprint that could present multiple avenues for a potential attacker. Key areas of concern include exposed services like the Remote Desktop Protocol (RDP) and the public availability of documents marked as "confidential."

## 2. Scope & Methodology

- **Target Domain:** `infosys.com`
- **Methodology:** The assessment was strictly passive, utilizing Open Source Intelligence (OSINT) techniques. Data was gathered from public search engines, DNS records, and specialized security search engines.
- **Tools Used:**
  - theHarvester
  - Recon-`ng` (with `hackertarget` module)
  - Shodan
  - Amass
  - Google Dorking

## 3. Findings

The following sections detail the information discovered during the assessment. For direct tool outputs and screenshots, please refer to **Appendix A: Evidence**.

### 3.1. Email Addresses

The `theHarvester` tool identified several email addresses associated with the `infosys.com` domain.

- **Emails Found:**
  - 0\_10\_@infosys.com
  - anny\_liu@infosys.com
  - arunacnewton@infosys.com
  - china\_freshers@infosys.com
  - connect-china@infosys.com
  - infy-rec\_helpdesk@infosys.com
  - infy\_zhaopin@infosys.com
  - instep\_team@infosys.com

**Impact:** These addresses could be used in targeted phishing campaigns or social engineering attacks against Infosys employees.

### 3.2. Domain & Subdomain Enumeration

A vast number of subdomains were discovered, indicating a wide digital presence.

- **Hosts Found:** theHarvester reported finding **845 hosts**.
- **Key Subdomains Identified (from Amass, Recon-ng, theHarvester):**
  - admin.infosys.com
  - blogs.infosys.com
  - forms.infosys.com
  - jamfadcs.infosys.com
  - oic.infosys.com
  - rec-test.infosys.com
  - usasbc01-ext.infosys.com
  - usasbc02-ext.infosys.com

**Impact:** Each subdomain represents a potential entry point. Subdomains like `rec-test` may have weaker security configurations than production environments, posing a significant risk.

### 3.3. IP Addresses & Network Infrastructure

Multiple IP addresses, netblocks, and Autonomous System Numbers (ASNs) were identified.

- **Identified IPs:**
  - infosys.com -> 35.71.178.178
  - usasbc01-ext.infosys.com -> 122.98.130.127
  - usasbc02-ext.infosys.com -> 122.98.118.127
  - jamfadcs.infosys.com -> 122.98.14.176
- **Identified ASNs:**
  - 38191 (Infosys Technologies Ltd)
  - 16509 (Amazon.com, Inc.)
  - 55410 (Vodafone Idea Ltd, IN)

**Impact:** This information maps out the company's network infrastructure and reveals its hosting partners (e.g., Amazon AWS).

### 3.4. Open Ports & Services (Shodan)

Shodan identified 13 internet-facing devices, primarily located in the United States and India.

- **Common Open Ports:** 443 (HTTPS), 25 (SMTP), 465 (SMTPTS).

- **High-Risk Open Ports:** 3389 (Remote Desktop Protocol - RDP) was identified on at least two devices.
- **Identified Technologies:** NGINX web servers, MailEnable SMTP servers.

**Impact:** Exposed RDP ports are a primary target for brute-force and ransomware attacks. If not properly secured with strong passwords, MFA, and access controls, they present a critical vulnerability.

### 3.5. Sensitive Information Exposure (Google Dorking)

Advanced Google searches revealed potentially sensitive data.

- **Confidential Documents:** A search for `site:infosys.com filetype:pdf "confidential"` returned several documents, including `enterprise-data-protection.pdf` and others related to cloud security and data analytics that contain the word "confidential".
- **Exposed Login Pages:** A search for `site:infosys.com inurl:login` identified a generic login portal and a related user manual.

**Impact:** The public availability of documents labeled "confidential" suggests a potential breakdown in data classification and handling procedures. Exposed login pages provide clear targets for credential stuffing and brute-force attacks.

## 4. Recommendations

Based on these passive findings, the following actions are recommended:

1. **Reduce Attack Surface:** Conduct an internal audit of all discovered subdomains. Decommission any that are no longer required, especially non-production environments like `rec-test`.
2. **Secure Exposed Services:** Immediately review the security of all devices with port 3389 (RDP) open. Enforce strong, unique passwords, enable Multi-Factor Authentication (MFA), and restrict access to trusted IP addresses only.
3. **Data Leakage Prevention:** Review all publicly accessible files on the `infosys.com` domain to ensure that no internal or sensitive information is inadvertently exposed. Implement a web application firewall (WAF) rule to block crawling of sensitive directories.
4. **Employee Training:** Enhance security awareness training for employees, focusing on the risks of phishing, using the discovered email address formats as examples.

## 5. Conclusion

The passive reconnaissance of `infosys.com` reveals a significant and varied external attack surface. The volume of subdomains, combined with exposed high-risk services and potentially sensitive documents, provides a fertile ground for a malicious actor to begin a more targeted attack. It is strongly recommended that the organization proceeds with a comprehensive vulnerability assessment and penetration test to actively identify and remediate the security weaknesses suggested by this report.

## Appendix A: Evidence

This appendix contains references to the screenshots captured during the assessment, which serve as evidence for the findings in Section 3.

### • EVD-01: Shodan Scan Results

- **Description:** Shodan dashboard showing 13 total results for `infosys.com`, with details on top countries (United States, India), open ports (443, 3389), and organizations.

13

Product Spotlight: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

TOP COUNTRIES



United States	7
India	5

TOP PORTS

443	7
3389	2
25	1
465	1
5985	1
More...	

TOP ORGANIZATIONS

Amazon Data Services India	5
Microsoft Corporation	2
TXNet Communications LLC	2
Unified Layer	2
Google LLC	1
More...	

TOP PRODUCTS

nginx	4
MailEnable smptd	2
OpenBSD	2

**Error** 40.118.228.234  
apimarketplace-gw.infosysapps.com  
Microsoft Corporation  
United States, San Jose  
cloud

**SSL Certificate**  
Issued By:  
- Common Name: DigiCert Global G2 TLS RSA SHA256 2020 CA1  
- Organization: DigiCert Inc  
Issued To:  
- Common Name: apimarketplace-gw.infosysapps.com  
- Organization: Infosys Limited  
Supported SSL Versions: TLSv1.2

**104.167.243.228**  
TXNet Communications LLC  
United States, Spring  
self-signed

**SSL Certificate**  
Issued By:  
- Common Name: VISFTP.v-infosys.com  
Issued To:  
- Common Name: VISFTP.v-infosys.com  
Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2

**35.226.160.84**  
84.160.226.35.bc.googleusercontent.com  
Google LLC  
United States, Council Bluffs  
cloud self-signed

**SSL Certificate**  
Issued By:  
- Common Name: can-dc.can.infosys.com  
Issued To:  
- Common Name: can-dc.can.infosys.com  
Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2

HTTP/1.1 404 Not Found  
Date: Mon, 01 Sep 2025 05:48:12 GMT  
Content-Type: text/html; charset=utf-8  
Content-Length: 243  
Connection: keep-alive  
Vary: Origin  
Access-Control-Allow-Origin: https://apimarketplace.infosysapps.com  
X-Content-Type-Options: nosniff  
X-Frame-Options: SAMEORIGIN  
X-XSS-...

Remote Desktop Protocol  
\x03\x00\x00\x13\x0e\x0d\x00\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00\x00  
Remote Desktop Protocol NTLM Info:  
OS: Windows Server 2022  
OS Build: 10.0.20348  
Target Name: V-INFOSYS  
NetBIOS Domain Name: V-INFOSYS  
NetBIOS Computer Name: VISFTP  
DNS Domain Name: v-infosys...  
...

Remote Desktop Protocol  
\x03\x00\x00\x13\x0e\x0d\x00\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00\x00  
Remote Desktop Protocol NTLM Info:  
OS: Windows Server 2022  
OS Build: 10.0.20348  
Target Name: CAN  
NetBIOS Domain Name: CAN  
NetBIOS Computer Name: CAN-DC  
DNS Domain Name: can.infosys.com  
...

- **EVD-02: theHarvester Scan Results**
  - **Description:** Console output from theHarvester showing 9 emails found and a partial list of 845 subdomains discovered.

```
[*] Emails found: 9
_____
'0_10_@infosys.com
 '@infosys.com
anny_liu@infosys.com
arunacnewton@infosys.com
china_freshers@infosys.com
connect-china@infosys.com
infy_rec_helpdesk@infosys.com
infyzhaopin@infosys.com
instep_team@infosys.com

[*] No people found.

[*] Hosts found: 845
_____
....infosys.com
Blrlsweb.infosys.com
ISGFAHXPUNSEZ.ad.infosys.com
ISGFANX2JPN.ad.infosys.com
ISGFANXAUS02.ad.infosys.com
ISGFANXAUSMEL05.ad.infosys.com
ISGFANXBBLRB06.ad.infosys.com
ISGFANXCHDSEZ02.ad.infosys.com
ISGFANXCHNB02.ad.infosys.com
ISGFANXCHNB04.ad.infosys.com
ISGFANXCHNMB05.ad.infosys.com
ISGFANXPUNB06.ad.infosys.com
a.infosys.com
aarohan.infosys.com
abcd.ad.infosys.com
abm.infosys.com
ad.infosys.com
admin.infosys.com
aginsightsqa.ad.infosys.com
agprodk.ad.infosys.com
aip1w.ad.infosys.com
akaashq.infosys.com
alumni.infosys.com
analytics.infosys.com
analyticsy.infosys.com
antispam.infosys.com
apievents.infosys.com
appec.infosys.com
arisbussrvv01u.ad.infosys.com
aseanns.ad.infosys.com
```

- **EVD-03: Recon-ng Scan Results**

- **Description:** Console output from Recon-ng's `hackertarget` module, listing resolved hosts and their corresponding IP addresses (e.g., `jamfadcs.infosys.com`).

```
SOURCE ⇒ infosys.com
[recon-ng][default][hackertarget] > run
```

```
INFOSYS.COM
```

```
[*] Country: None
[*] Host: infosys.com
[*] Ip_Address: 35.71.178.178
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: jamfadcs.infosys.com
[*] Ip_Address: 122.98.14.176
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: oic.infosys.com
[*] Ip_Address: 204.74.99.103
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: usasbc01-ext.infosys.com
[*] Ip_Address: 122.98.130.127
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: usasbc02-ext.infosys.com
[*] Ip_Address: 122.98.118.127
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
```

- **EVD-04: Google Dorking for Confidential Documents**
  - **Description:** Google search results for `site:infosys.com filetype:pdf "confidential"`, showing multiple PDF documents indexed by the search engine.

The screenshot shows a Google search results page with the following details:

**Search Query:** site:infosys.com filetype:pdf "confidential"

**Filter:** All

**Results:**

- Azure Confidential Ledger (ACL) For Enhanced Privacy**  
Azure Confidential Ledger is an offering from the Microsoft suite that comes in with an extra layer of security and scalability on top of blockchain.  
4 pages
- Data Analytics Services & Solutions**  
Proprietary and Confidential. ISG Confidential. © 2018 Information Services Group, Inc. All Rights Reserved. ISG (Information Services Group) (NASDAQ: III) is ...
- Improving Cloud Security With Efficient Cloud Identity & ...**  
These policies then help to magnify identity related risk score by defining potential risk of escalated identities having access to confidential data.
- enterprise-data-protection.pdf**  
IEDPS is a one-stop solution for protection of confidential, sensitive, private, and personally identifiable information within enterprise repositories ...  
4 pages
- Enabling Innovation in Banking**  
©2017 Discover Financial Services - Confidential and Proprietary - Do not copy or distribute. 1. ©2017 Discover Financial Services - Confidential and ...

- **EVD-05: Google Dorking for Login Pages**
  - **Description:** Google search results for site:infosys.com inurl:login, identifying a "Sign in" portal and a "User Manual Guide" in PDF format.

Google

site:infosys.com inurl:login

All Mode All Images Shopping Videos News Short videos More Tools

**Infosys**  
https://career.infosys.com › login

**Sign In**

**Infosys**  
https://www.infosys.com › generic-login

**User Manual Guide For:**  
To log in into the portal, you need to enter a valid email to receive an OTP and click "Next" button. Step 01. Step 01. Logging Into The Portal ...  
3 pages

*In order to show you the most relevant results, we have omitted some entries very similar to the 2 already displayed.  
If you like, you can repeat the search with the omitted results included.*

- **EVD-06: Amass Scan Results**

- **Description:** Console output from Amass showing detailed passive DNS enumeration, including CNAME records, A records, and associated netblocks/ASNs.

```
└$ amass enum -passive -d infosys.com
infosys.com (FQDN) → ns_record → udns2.cscdns.uk (FQDN)
infosys.com (FQDN) → ns_record → udns1.cscdns.net (FQDN)
blogs.infosys.com (FQDN) → cname_record → blogs.infosys.com.edgekey.net (FQDN)
ir-pan-info.infosys.com (FQDN) → cname_record → ir-pan-info.infosys.com.edgekey.net (FQDN)
de-living-labs.infosys.com (FQDN) → cname_record → de-living-labs.infosys.com.edgekey.net (FQDN)
forms.infosys.com (FQDN) → cname_record → d3aha9pq4nk78j.cloudfront.net (FQDN)
itgateway.infosys.com (FQDN) → cname_record → itgateway.infosys.com.edgekey.net (FQDN)
autodiscover.infosys.com (FQDN) → cname_record → autodiscover.infosys.com.infycorp.akadns.net (FQDN)
rec-test.infosys.com (FQDN) → cname_record → d26dzko45z9eg9.cloudfront.net (FQDN)
livinglabs-virtual.infosys.com (FQDN) → cname_record → livinglabs-virtual.infosys.com.edgekey.net (FQDN)
usasbc01-ext.infosys.com (FQDN) → a_record → 122.98.130.127 (IPAddress)
edge.infosys.com (FQDN) → cname_record → edge.infosys.com.infycorp.akadns.net (FQDN)
blrketeamssbc01.infosys.com (FQDN) → a_record → 123.63.43.186 (IPAddress)
stsakaash.infosys.com (FQDN) → cname_record → stsakaash.infosys.com.edgekey.net (FQDN)
plamail.infosys.com (FQDN) → cname_record → plamail.infosys.com.infycorp.akadns.net (FQDN)
122.98.128.0/20 (Netblock) → contains → 122.98.130.127 (IPAddress)
123.63.43.0/24 (Netblock) → contains → 123.63.43.186 (IPAddress)
38191 (ASN) → managed_by → INFOSYS-AS Infosys Technologies Ltd (RIROrganization)
38191 (ASN) → announces → 122.98.128.0/20 (Netblock)
55410 (ASN) → managed_by → VIL-AS-AP Vodafone Idea Ltd, IN (RIROrganization)
55410 (ASN) → announces → 123.63.43.0/24 (Netblock)
jamfadcs.infosys.com (FQDN) → a_record → 122.98.14.176 (IPAddress)
216.137.39.0/24 (Netblock) → contains → 216.137.39.33 (IPAddress)
216.137.39.0/24 (Netblock) → contains → 216.137.39.20 (IPAddress)
216.137.39.0/24 (Netblock) → contains → 216.137.39.26 (IPAddress)
216.137.39.0/24 (Netblock) → contains → 216.137.39.62 (IPAddress)
122.98.8.0/21 (Netblock) → contains → 122.98.14.176 (IPAddress)
2600:9000:2085::/48 (Netblock) → contains → 2600:9000:2085:a600:4:ebca:1a40:93a1 (IPAddress)
2600:9000:2085::/48 (Netblock) → contains → 2600:9000:2085:2c00:4:ebca:1a40:93a1 (IPAddress)
2600:9000:2085::/48 (Netblock) → contains → 2600:9000:2085:8a00:4:ebca:1a40:93a1 (IPAddress)
2600:9000:2085::/48 (Netblock) → contains → 2600:9000:2085:c00:4:ebca:1a40:93a1 (IPAddress)
2600:9000:2085::/48 (Netblock) → contains → 2600:9000:2085:cc00:4:ebca:1a40:93a1 (IPAddress)
2600:9000:2085::/48 (Netblock) → contains → 2600:9000:2085:ce00:4:ebca:1a40:93a1 (IPAddress)
2600:9000:2085::/48 (Netblock) → contains → 2600:9000:2085:4400:4:ebca:1a40:93a1 (IPAddress)
2600:9000:2085::/48 (Netblock) → contains → 2600:9000:2085:c400:4:ebca:1a40:93a1 (IPAddress)
38191 (ASN) → announces → 122.98.8.0/21 (Netblock)
0 (ASN) → managed_by → Not routed (RIROrganization)
0 (ASN) → announces → 216.137.39.0/24 (Netblock)
16509 (ASN) → managed_by → AMAZON-02 - Amazon.com, Inc. (RIROrganization)
16509 (ASN) → announces → 2600:9000:2085::/48 (Netblock)
```

- **EVD-07: theHarvester XML Output**

- **Description:** The raw XML output file saved from theHarvester, confirming the emails and hosts discovered during the scan.

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
--<theHarvester>
  <cmd>-d infosys.com -l 500 -f myresults.html -b all</cmd>
  <email>'0_10_@infosys.com</email>
  <email> '@infosys.com</email>
  <email>anny_liu@infosys.com</email>
  <email>arunacnewton@infosys.com</email>
  <email>china_freshers@infosys.com</email>
  <email>connect-china@infosys.com</email>
  <email>infy_rec_helpdesk@infosys.com</email>
  <email>infyzhaopin@infosys.com</email>
  <email>instep_team@infosys.com</email>
  <host>www.infosys.com</host>
  <host>....infosys.com</host>
-<host>
  <ip>122.98.118.127</ip>
  <hostname>usasbc02-ext.infosys.com</hostname>
-</host>
--<host>
  <ip>61.95.162.151</ip>
  <hostname>infosysaim.infosys.com</hostname>
-</host>
-<host>
  <ip>122.98.14.31</ip>
  <hostname>kecgate05.infosys.com</hostname>
-</host>
--<host>
  <ip>122.98.130.127</ip>
  <hostname>usasbc01-ext.infosys.com</hostname>
-</host>
--<host>
  <ip>122.98.14.32</ip>
  <hostname>kecgate02.infosys.com</hostname>
-</host>
-<host>
```

Mouse pointer inside or press Ctrl+G.