

# 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 (SMTPS).

- **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.

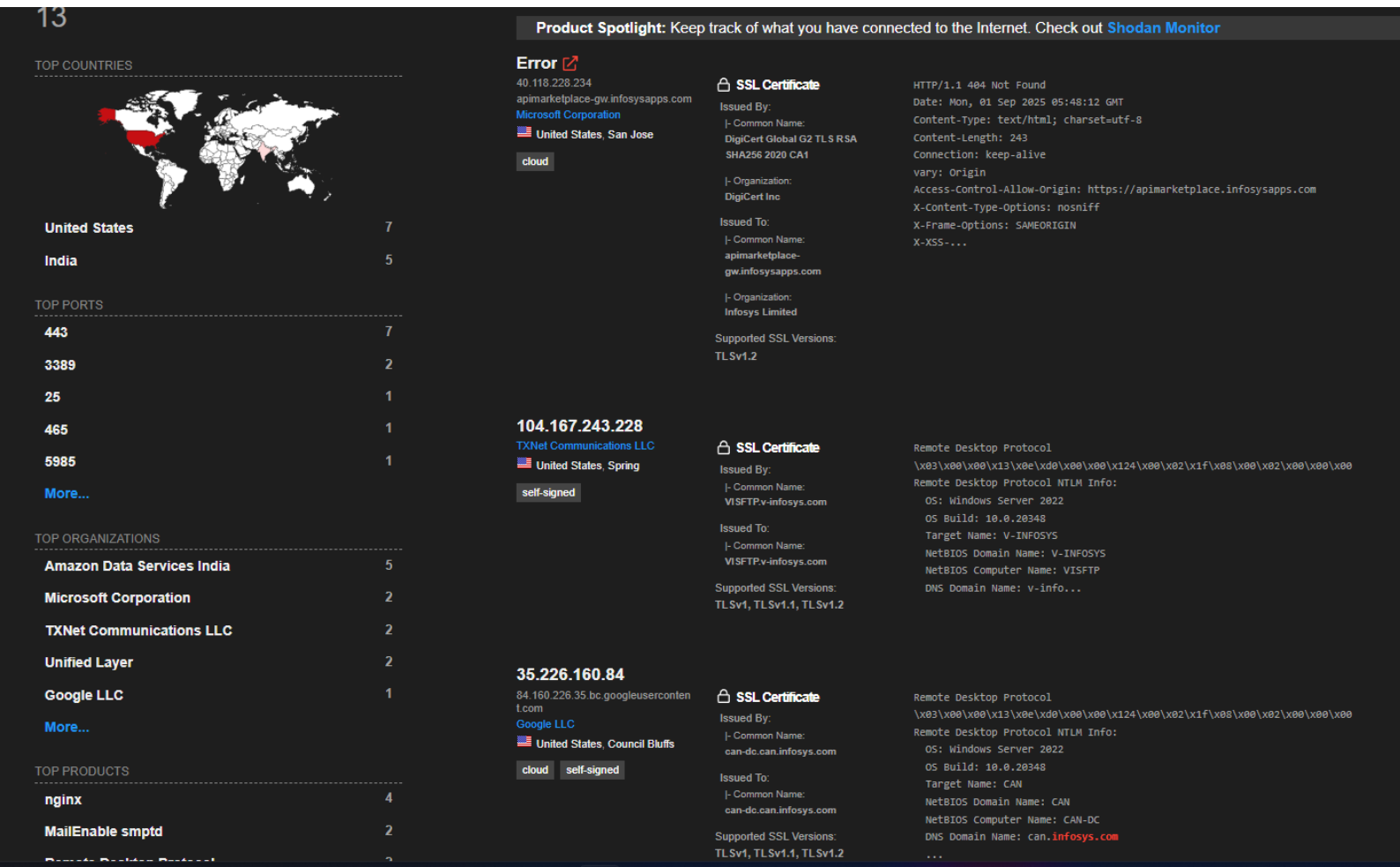
## 5. Conclusion

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.



- **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  
ISGFANXPUNSEZ.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  
aaroan.infosys.com  
abcd.ad.infosys.com  
abm.infosys.com  
ad.infosys.com  
admin.infosys.com  
aginsightsqa.ad.infosys.com  
agprodk.ad.infosys.com  
aiplw.ad.infosys.com  
akaashq.infosys.com  
alumni.infosys.com  
analytics.infosys.com  
analyticy.infosys.com  
antispam.infosys.com  
apievents.infosys.com  
appec.infosys.com  
arisbussrvv01u.ad.infosys.com  
aseapps.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.


---




site:infosys.com filetype:pdf "confidential"

✕ | 🔊 | 🖨️ | 🔍


AI Mode **All** Images News Videos Short videos Forums More ▾ Tools ▾

 Infosys  
https://www.infosys.com › insights › documents PDF ⋮


**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

 Infosys  
https://www.infosys.com › insights › documents PDF ⋮


**Data Analytics Services & Solutions**  
Proprietary and **Confidential**. ISG **Confidential**. © 2018 Information Services Group, Inc. All Rights Reserved. ISG (Information Services Group) (NASDAQ: III) is ...

 Infosys  
https://www.infosys.com › services › insights › i... PDF ⋮

**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.

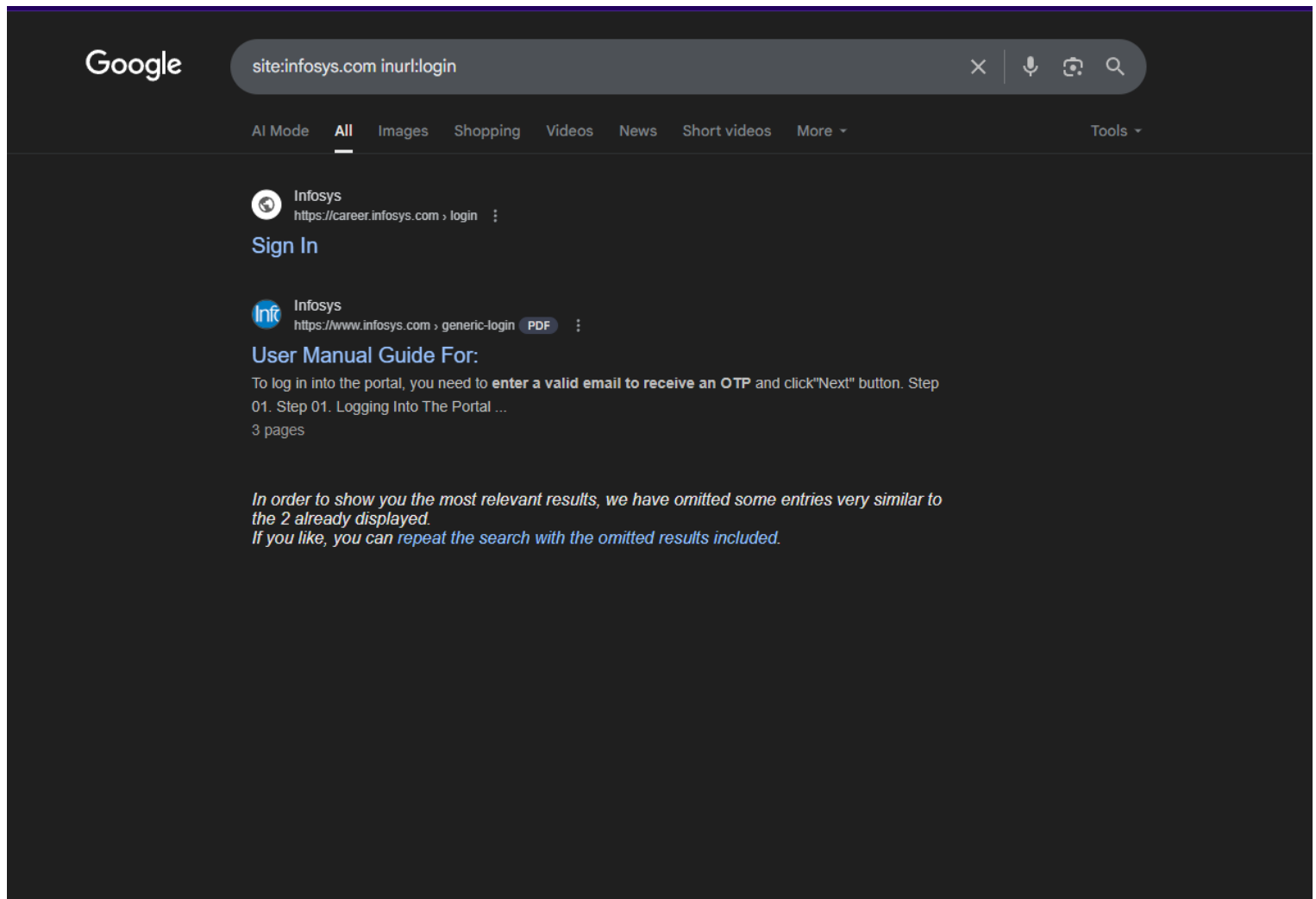
 Infosys  
https://www.infosys.com › it-services › documents PDF ⋮

**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

 Infosys  
https://www.infosys.com › images › presentation PDF ⋮

**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.





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

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

```
L$ 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)
blrkecteamssbc01.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.

```

- <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>infyzaopin@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>

```

ouse pointer inside or press Ctrl+G.