Appendix A:
Assessment Team Analysis of Speridian Server Locations

Speridian, in their Response to CMS' Notice of Determination dated June 12, 2025, disputed that two specific IP addresses that CMS cited as evidence of Speridian failing to restrict access of feature sets to US-based IP addresses were in fact non-US-based IP addresses. Speridian contends that using a service called MaxMind, these two IP addresses are shown as located in the US. A screenshot of the MaxMind report was provided in their response.

The Assessment Team (MITRE and KPMG) were asked to review this rebuttal, and have determined that their rebuttal is not persuasive for the following reasons:

1) At the time of the investigation, KPMG found that the two IP addresses in question (**199.34.21.146** and **199.34.21.148**) had domain names associated with Speridian Companies and that while the certificate authority (GoDaddy.com) was in the US, the servers themselves were physically located in India. (*See point #2: Certificate Issuer*)

2) Also, at the time of the investigation, KPMG used Shodan lookup to take screenshots of the two IP addresses, which showed that these addresses were Windows servers hosting email services in India and associated with Sperdian (*See point #4: Services (open ports) and Domains*).

    a. Note that the certificates associated with these two IP addresses were set to expire in February 2025, which may indicate that they are no longer used by Speridian. Shodon Lookup does not currently return any information for these IP addresses.

3) While not currently resolving to the Speridian companies, the IP addresses themselves are still located in India today. Using other geolocation services other than MaxMind, which based on KPMG's experience is not 100% reliable, these IP addresses show up as being hosted in India *(See point #1: Geolocation services)*

4) Further, doing a traceroute on the two IP addresses also shows that the final hop to those addresses are located in India *(See point #3: Traceroute)*

5) Finally, when performing a Shodon search on domains related to Speridian.com, two other IP addresses geolocated in India (**121.242.90.65** and **121.242.120.116**) are showing up as having the same domains and system information as what was previously associated with IP address 199.34.21.146 and 199.34.21.148) (*See point #4: Services (open ports) and Domains*).

Source Content from KPMG technical assessment:

1. **Geolocation services:**

In our experience MaxMind is not a 100% reliable service in terms of geolocating IP addresses. We typically use a variety of services that report additional details about a specific IP address and the system behind it, to determine where something is located geographically. With a quick check, the original IP addresses (199.34.21.146 and 199.34.21.148) are still reported as geolocated in India in the following services:

a) 199.34.21.146:

   a. https://www.ip2location.com/demo/199.34.21.146
   b. https://platform.censys.io/hosts/199.34.21.146
   c. https://ipgeolocation.io/what-is-my-ip/199.34.21.146
   d. https://ipinfo.io/199.34.21.146

b) 199.34.21.148:

   e. https://www.ip2location.com/demo/199.34.21.148
   f. https://platform.censys.io/hosts/199.34.21.148
   g. https://ipgeolocation.io/what-is-my-ip/199.34.21.148
   h. https://ipinfo.io/199.34.21.148

2. **Certificate issuer:**

At the time of the investigations, these two IP addresses resolved to domain names associated with Speridian companies (speridian.com, mail.speridian.com, mail.truecoverage.com, etc.). The SSL/TLS certificates issued for these domain names, were issued by a Certificate Authority (CA) in the United States: GoDaddy. Note that the certificate that was associated with these domains was set to expire in February 2025. Some IP geolocation services might mistakenly associate the origin of the Certificate Authority (US) with the physical location of the server (India).

- https://www.virustotal.com/gui/ip-address/199.34.21.146/details
- https://www.virustotal.com/gui/ip-address/199.34.21.148/details

Data: Version: V3

Serial Number: aa8e448bf8ec7d83

Thumbprint: af209303a975d04b7037be6be8d5e315f4cffcfe

Signature Algorithm:

Issuer: C=US ST=Arizona L=Scottsdale O=GoDaddy.com, Inc. OU=http://certs.godaddy.com/repository/ CN=Go Daddy Secure Certificate Authority - G2

Validity

Not Before: 2024-08-09 08:18:13

Not After: 2025-02-01 09:30:01

Subject: CN=mail.speridian.com

3. **Traceroute information:**

A traceroute is a tool that maps path data takes from a computer to a specific destination on the internet (IP address), showing each "stop" (or router) along the way.

When doing a traceroute from my computer to either of these IP addresses, the last “hop” is still an IP address geolocated in India (154.210.186.131):

traceroute 199.34.21.146

traceroute to 199.34.21.146 (199.34.21.146), 64 hops max, 40 byte packets

1 192.168.1.1 (192.168.1.1) 3.527 ms 2.695 ms 2.115 ms

2 172.30.48.1 (172.30.48.1) 16.383 ms 16.435 ms 17.126 ms

3 216.80.78.69 (216.80.78.69) 15.259 ms 17.241 ms 14.624 ms

4 * * *

5 * * *

6 hge0-0-0-21.edge1.dca-eqnx.va.bb.astound.net (75.76.132.122) 31.789 ms

hge0-0-0-8.edge1.dca-eqnx.va.bb.astound.net (207.172.18.137) 30.100 ms

hge0-0-0-1.edge1.dca-eqnx.va.bb.astound.net (207.172.19.86) 34.320 ms

7 eqix-dc2.telstra.com (206.126.237.239) 30.625 ms 29.406 ms 29.233 ms

8 i-90.unse-core01.telstraglobal.net (202.84.252.213) 45.998 ms 39.725 ms 36.308 ms

9 i-1098.eqnx-core02.telstraglobal.net (202.84.252.245) 109.822 ms 100.354 ms 95.395 ms

10 i-15108.sgcn-core01.telstraglobal.net (202.84.136.1) 268.525 ms

i-25108.sgcn-core01.telstraglobal.net (202.84.143.121) 277.871 ms

i-15108.sgcn-core01.telstraglobal.net (202.84.136.1) 267.361 ms

11 i-25108.sgcn-core01.telstraglobal.net (202.84.143.121) 272.961 ms 279.579 ms 271.803 ms

12 i-91.istt04.telstraglobal.net (202.84.224.197) 283.818 ms 271.802 ms 274.756 ms

13 unknown.telstraglobal.net (210.57.38.115) 267.693 ms

unknown.telstraglobal.net (210.57.38.113) 278.281 ms 273.165 ms

14 103.198.140.88 (103.198.140.88) 269.941 ms

49.45.4.83 (49.45.4.83) 266.371 ms

49.45.4.87 (49.45.4.87) 279.815 ms

15 103.198.140.65 (103.198.140.65) 285.315 ms

103.198.140.171 (103.198.140.171) 422.686 ms

49.44.220.10 (49.44.220.10) 281.093 ms

16 * * *

17 49.44.218.70 (49.44.218.70) 293.596 ms 302.049 ms 288.808 ms

18 154.210.186.131 (154.210.186.131) 303.309 ms 291.391 ms 298.507 ms

19 * * *

20 * * *

21 * * *

22 * * *

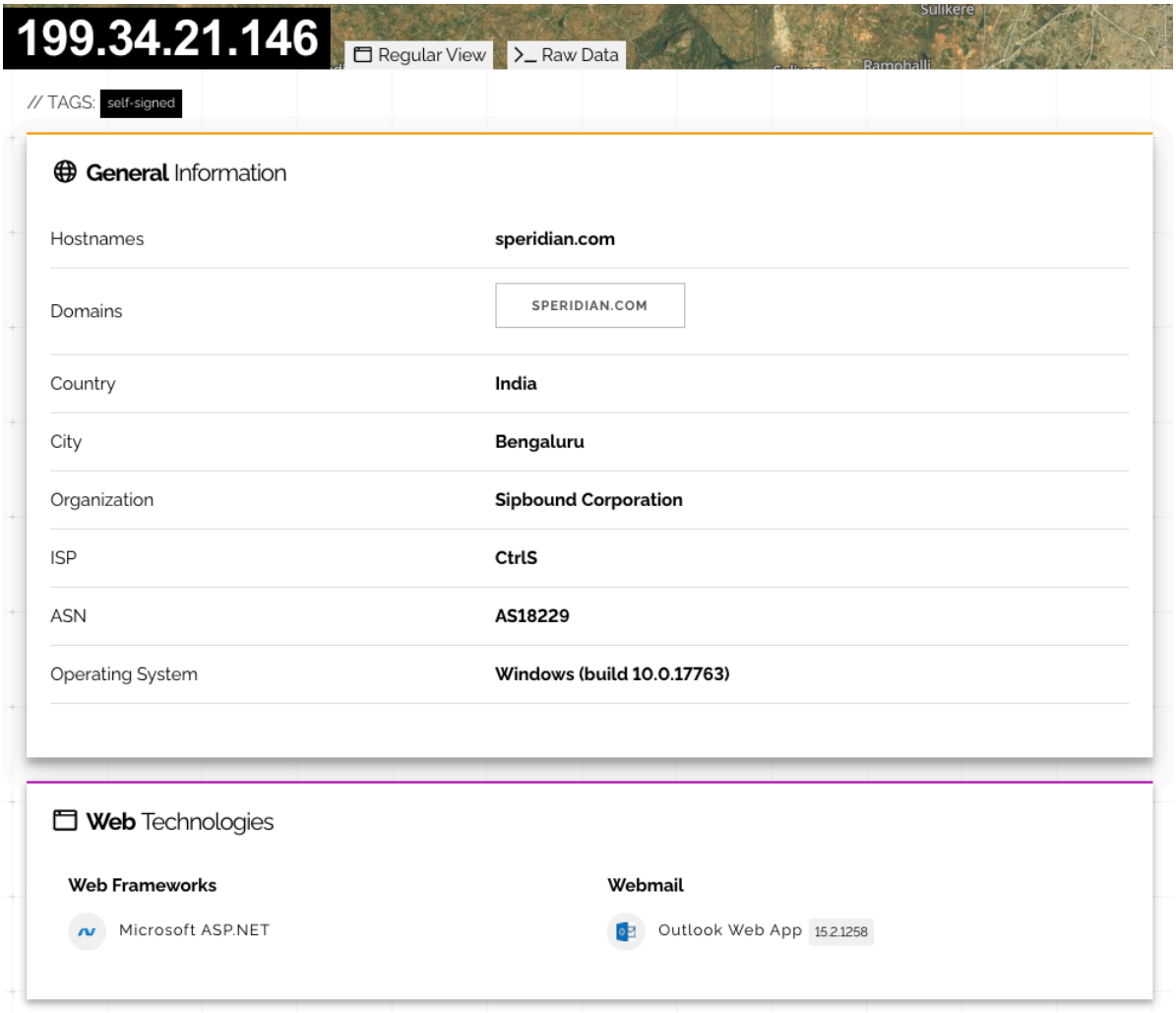
23 * * *

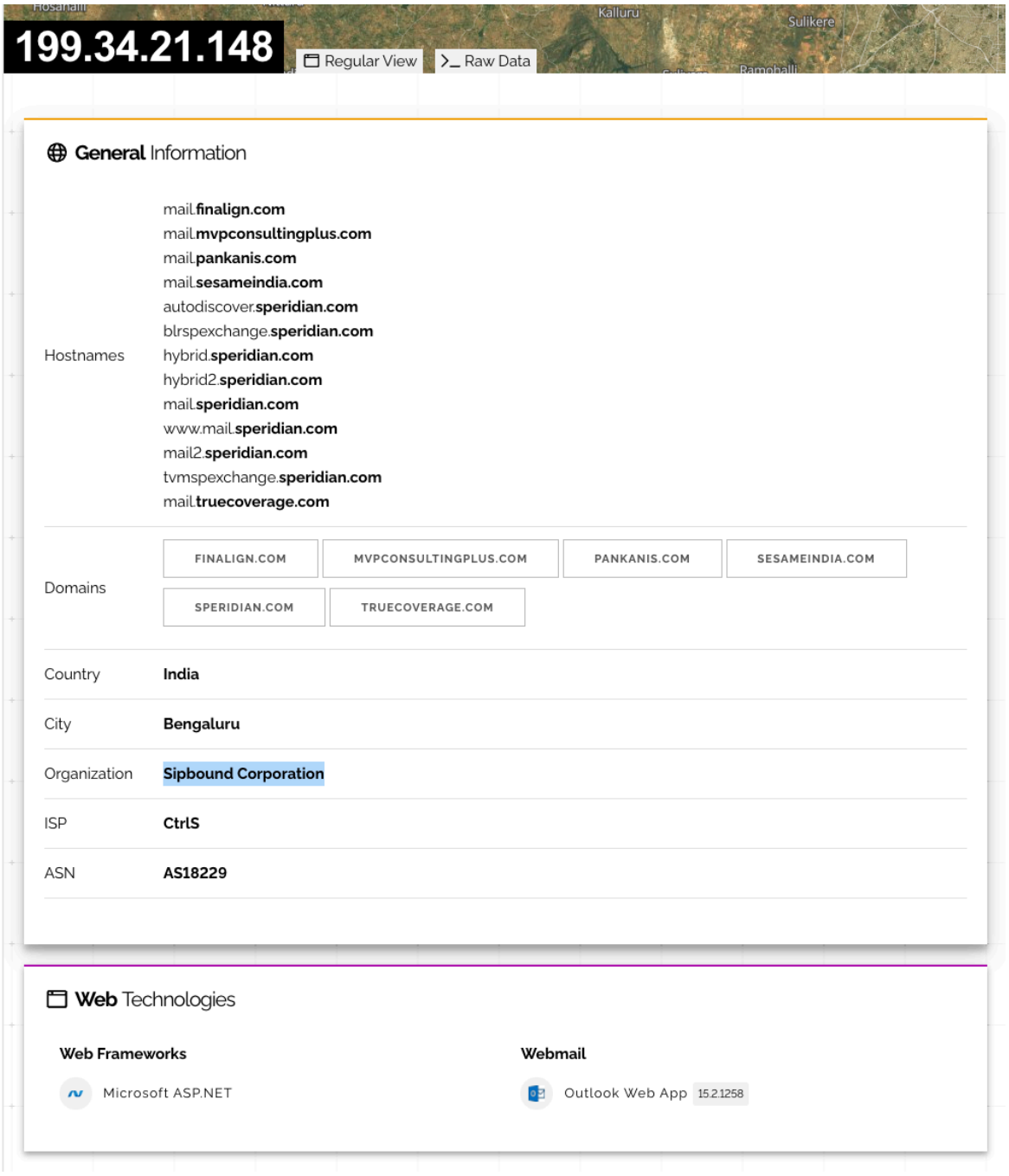
24 * * *

25 * * *

4. **Services (open ports) and domains:**

At the time of the investigation and reporting, we took screenshots of various resolutions of the IP addresses in question. Below are the screenshots we took from the Shodan lookup service back in November 2024. In the screenshots you can see that these IP addresses were associated Windows systems hosting email services (Microsoft Exchange servers) related to a variety of Speridian domains geolocated in India. However, today, these two IP addresses no longer return results in Shodan.





Separately, when doing a search in Shodan for services related to the Speridian domain "speridian.com", the search returns new IP addresses geolocated in India for similar Microsoft Exchange servers as the ones previously recorded: https://www.shodan.io/search?query=hostname%3A%22speridian.com%22+country%3A%22IN%22

- 121.242.90.65: associated with the same domains and system information as previously recorded on 199.34.21.146
- 121.242.120.116: associated with the same domains and system information as previously recorded on 199.34.21.148