Open Source Intelligence Techniques:

Delta Air Lines

Table of Contents

Summary

In this report I explore an OSINT investigation on Delta Air Lines, using techniques such as WhoIs, NSLookup, DIG, Recon-ng, and other frameworks which lend insight into the information readily accessible through the internet.

Methodology

i. List of OSINT techniques used: WhoIS, NSLookup, DIG, MXToolbox, Recon-ng, The Harvester, Maltego, Shodan, Spiderfoot

ii. Description of techniques used:

To accomplish this open source intelligence report, several methods were used. The first method, WhoIS, queries databases based on information collected when a person or organization registers a domain name or updates their DNS settings (domain.com). The WhoIS tool is important in maintaining the integrity of an organization's domain name and website ownership; however, the information gathered from the query can be used maliciously, as detailed in the next section. The source searched was delta.com, and the command used was whois delta.com.

The second tool used was NSLookUp, and the command used was nslookup delta.com. This tool reveals the IP address of the delta.com domain, and additional address information.

The third tool, DIG, was used to retrieve information such as the IP addresses, name servers, and mail servers associated with the domain. The source searched was delta.com, and the command used was dig delta.com. A benefit of this tool is that it uses OS resolver libraries, rather than NSLookup which uses internal libraries. From a security standpoint, since OS resolver libraries are frequently updated and maintained by the operating system vendor, the DIG tool receives patches simultaneously along with the rest of the system. Consequently, DNS

lookups performed using DIG are less susceptible to vulnerabilities; however, both tools were useful in the context of this investigation. The DIG tool also generally provided more information in comparison to the NSLookUp tool.

The MXtoolbox was leveraged in this investigation to evaluate whether the mail eXchange records of the domain delta.com were set up correctly, and to confirm that the domain and related IP addresses were not blacklisted, and also were protected against spoofing attacks. The online tool, found at mxtoolbox.com, was used. Specific tests that were performed included MX lookup, DNS blacklist lookup, SPF Record check, and DMARC Record check.

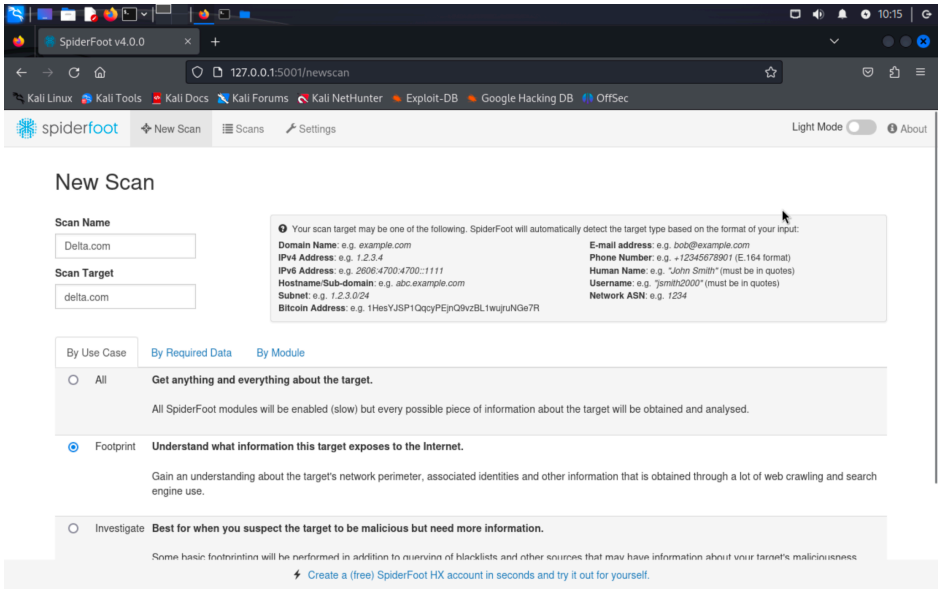
Recon-ng was used to obtain results from several open resources; the command used was recon-ng, in coordination with the *hackertarget* module. An HTML report was then generated for the purpose of this investigation, although it was limited in identifying underlying vulnerabilities in the delta.com domain.

The Harvester was used to collate subdomain names, email addresses, virtual hosts, and open ports. The command used was theHarvester -d delta.com -l 500 -b bing. A limitation of this tool is that it does not recognize Google as an acceptable source to search through for details, so only Bing was used. The command "all," which should search all available search engines, was also not recognized.

Maltego was used to gather general, extensive information about Delta, and the results from this tool were presented in the form of a tree graph. Details obtained from this tool included websites, MX records, snapshots, people, email addresses, and other information. However, not all the information provided seemed relevant in identifying vulnerabilities associated with the delta.com domain.

The Shodan tool was used briefly, with the IP address obtained earlier from the NSLookUp and DIG tools. The commands used were shodan host 204.74.99.103, and shodan domain delta.com. A limitation of this tool was, again, identifying and filtering relevant data.

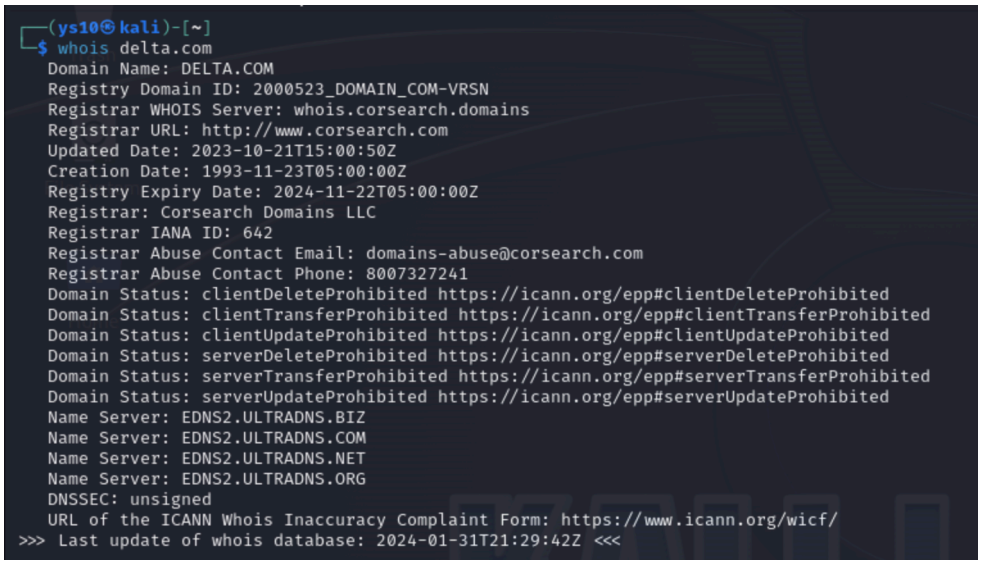
The final tool used was Spiderfoot, which automates over 100 queries, searching for email addresses, IP addresses, domains, phone numbers, and more data (nixintel.info). Commands were used to install the GUI. The scan was run on the delta.com domain. A benefit of this tool is it defines search tools against clear criteria; however, it took significantly longer to compile data in comparison to the other OSINT tools used. The "footprint" option was selected, in order to obtain information about delta.com's network perimeter, associated identities, and relevant information:



Naturally, the limitation of this option is that it only scans information exposed to the internet by delta.com, so hidden vulnerabilities may have been overlooked.

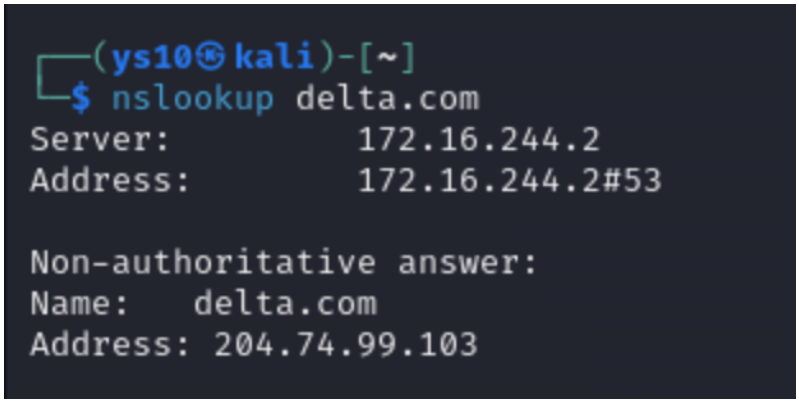
Findings

WhoIS:



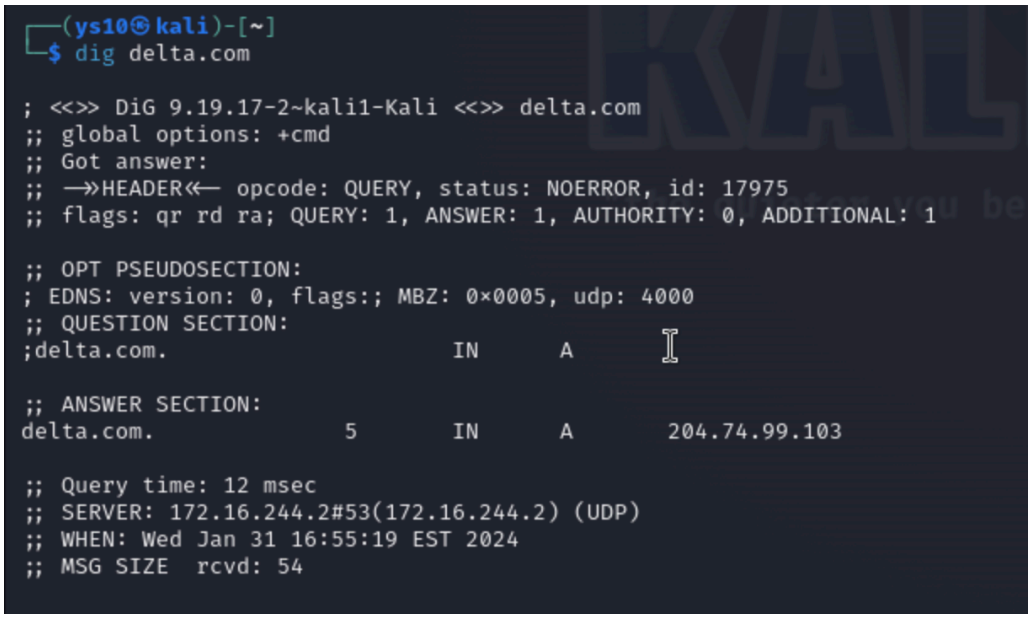
The output of the query (whois delta.com) reveals the domain name was registered by Corsearch Domains LLC, the domain was created on 11/23/1993 at 05:00:00, and the domain will expire on 2024-11-22 at 05:00:00. In the event of abuse, the registrar has a phone number and email address as well, disclosed in the output.

NSLookUp:



This command returns the domain name (delta.com), the IP address associated with the domain (204.74.99.103), the DNS server used to perform the query (172.16.244.2), and the IP address of this DNS server (172.16.244.2#53)

DIG:



This command corroborates the information found in NSLookup while providing some new insights. The IP address associated with the domain delta.com is 204.74.99.103. The DNS record type is A, and the DNS server used to perform the query is 172.16.244.2#53.

MXToolBox:

Results obtained from the MXToolBox reveal the delta.com domain has a valid DMARC record configured, a DMARC quarantine/reject policy enabled, and a published DNS record. The toolbox reveals the email provider for delta.com is “Proofpoint.” The DNSBL lookup option was also run on this domain, and delta.com is not recorded on any DNS-based blacklists. The third test run in the MXToolBox was an SPF record check; we find a valid SPF version is found. Subsequently, a valid DMARC record was found. Screenshots of all these MXToolBox results are included in appendices.

Recon-ng

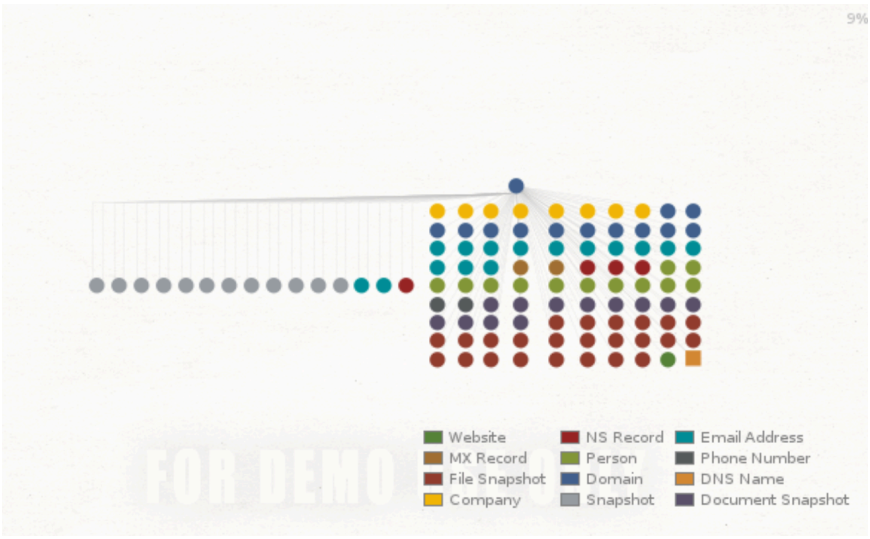
An HTML Recon-ng reconnaissance report for delta.com was prepared, and is included in the Appendices section of this report. This test reveals no known vulnerabilities associated with the delta.com domain, along with no open ports, netblocks, or leaks.

The Harvester

Searching through Bing using the Harvester tool revealed no IP addresses, emails, or hosts found for the target domain delta.com. As mentioned in the "Methodology" section, a limitation of these results is the test was only run with Bing, as other search engines did not return any results.

Maltego

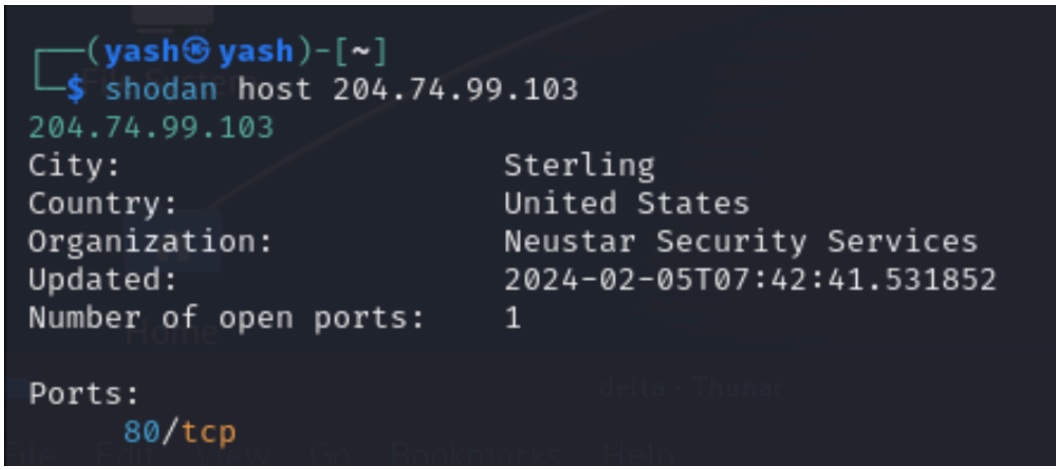
The Maltego tool was used to explore the delta.com domain's infrastructure, and present relationships between entities in the network. Details obtained included related websites, mail exchanger (MX) records, files, snapshots, and profiles including email addresses and phone numbers of employees and entities determined to have some connection with delta.com.



These results will be scrutinized further in the “Analysis” section to follow.

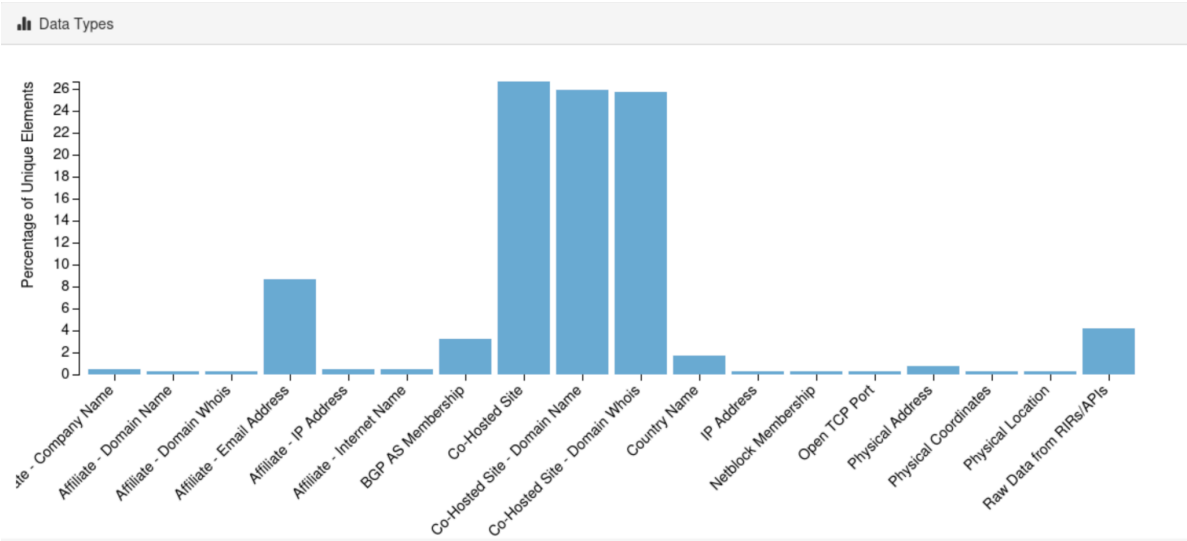
Shodan

The Shodan tool was used to obtain information about the delta.com domain and the IP address obtained previously using tools covered. This tool reveals open ports, the city, country, and the organization associated with the IP address.



Spiderfoot

The results from Spiderfoot provided a wide range of insights into the delta.com server, revealing one open port (substantiating other tests), and several co-hosted sites linked to delta.com. The findings are presented in the graph below, with an analysis to follow:



Furthermore, the "correlations" option was used to determine outlier countries associated with data elements in the network:

Delta scan FINISHED

Summary | Correlations | Browse | Graph | Scan Settings | Log

Correlation	Risk	Data Elements
Outlier country found: Australia	INFO	6
Outlier country found: Canada	INFO	1
Outlier country found: China	INFO	1
Outlier country found: Denmark	INFO	1
Outlier country found: Germany	INFO	1
Outlier country found: United Kingdom	INFO	2

Analysis

While the WhoIS record helps maintain the integrity of the delta.com domain name, it may be exploited by malicious actors to perform social engineering attacks. It is therefore imperative for the reader to be aware of the information that is available about the delta.com domain through the WhoIS command, as these credentials can be used to facilitate social engineering campaigns.

While the DIG command provides more information to a malicious actor than NSLookup, the NSLookup command does reveal the DNS server used to perform the query, and the IP address of that server. While this information simply being present is not a cause for concern, it can potentially be exploited through a phishing campaign or a denial-of-service attack, given the IP addresses of both the delta.com domain and the DNS server are present. The reader should be aware that the DIG tool corroborates the information obtained from NSLookup.

The Maltego tool was used on the domain delta.com, to identify people and entities reachable from the domain. Certain employee names appeared, and while these employees are not executives at the company, they may be targeted in social engineering campaigns as their names, personal email addresses, and in some instances phone numbers appeared in the Maltego search. From the search, an attacker can also learn that the delta.com domain is associated with VeriSign Global Registry, and with CorSearch Domains LLC - both accredited registry services. While the WhoIS tool indicates CorSearch is the registrar of the domain, a malicious actor may further investigate the connection to VeriSign.

The Shodan and Spiderfoot tools both report one open port, which was overlooked in the Recon-ng report; this discrepancy may be exploited by a malicious actor. Moreover, the scan conducted using Spiderfoot revealed six outlier countries which data elements in the delta.com

domain were associated with. The Recon-ng report does, however, reveal 500 hosts, which may open the door to exploit attempts.

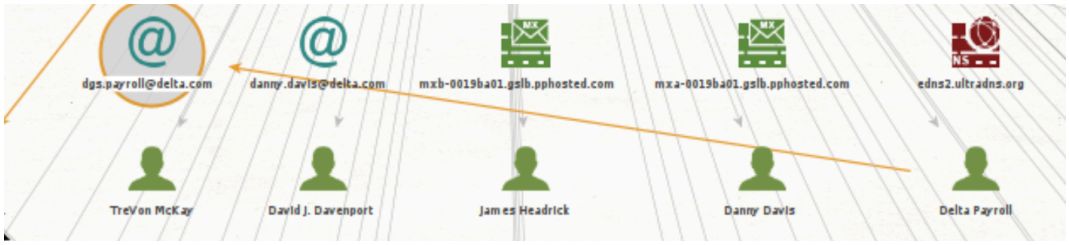
Recommendations

It is highly recommended for the CTO of Delta to peruse the information presented through the course of this report to either obtain or refresh an understanding of the information present through OSINT techniques. A possible social engineering campaign launched against Delta Air Lines may be initiated by a malicious actor claiming to be an employee of Corsearch, the registrar of the delta.com domain, which WhoIS indicates. The malicious actor may claim they received an email relating to an abuse, sent to domains-abuse@corsearch.com, which is also revealed in the WhoIS output, and may use this position to take advantage of one or several employees.

In addition to being aware of the social engineering risks, the reader should be cautious of the one open port reported in the Shodan and Spiderfoot findings. Since open ports may be exploited by malicious actors, it is highly recommended that this open port be regularly monitored, and patched should vulnerabilities be discovered. While the Recon-ng report did not reveal any open ports, it is important to stay vigilant in preparing against open port vulnerabilities.

The Maltego tool revealed names of employees associated with the delta.com domain, and more concerningly, “Delta Payroll” appeared among other employees, and an email address

was associated with this profile: dgs.payroll@delta.com.



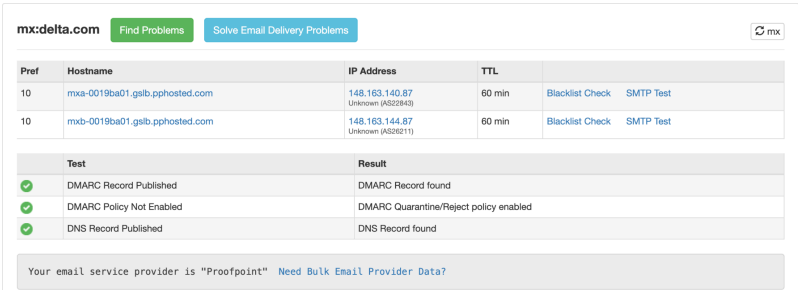
This email address may invite an attack on Delta's payroll, which may have immense consequences for a company of Delta's size. It is highly recommended for this email address to be monitored, and if this address is that of a mailing list, to remind all members of that mailing list to flag suspicious incoming emails.

Six outlier countries were found associated with data elements in the delta.com domain; activity in these outlier countries should be monitored closely, and in the event suspicious activity should occur in relation to any data elements associated with these countries, incoming traffic from these sources should be evaluated first.

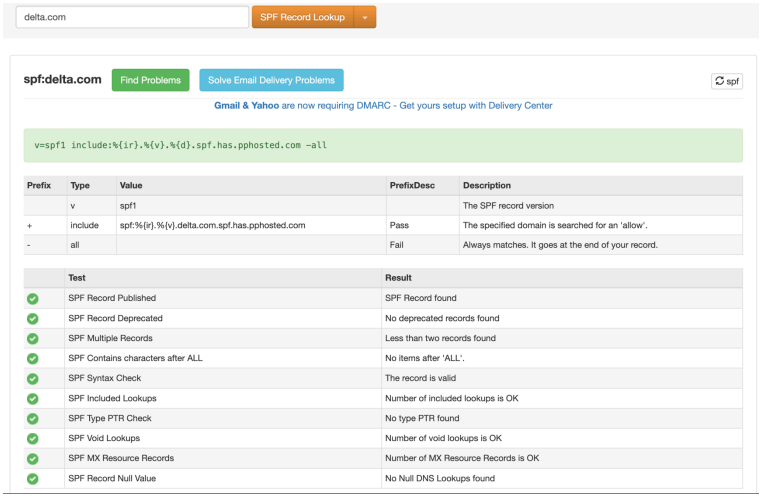
Ultimately, Delta Air Lines is maintaining a relatively high standard of cyber hygiene and security, as revealed using tools such as MXToolBox, recon-ng, Shodan, and Spiderfoot.

Appendices

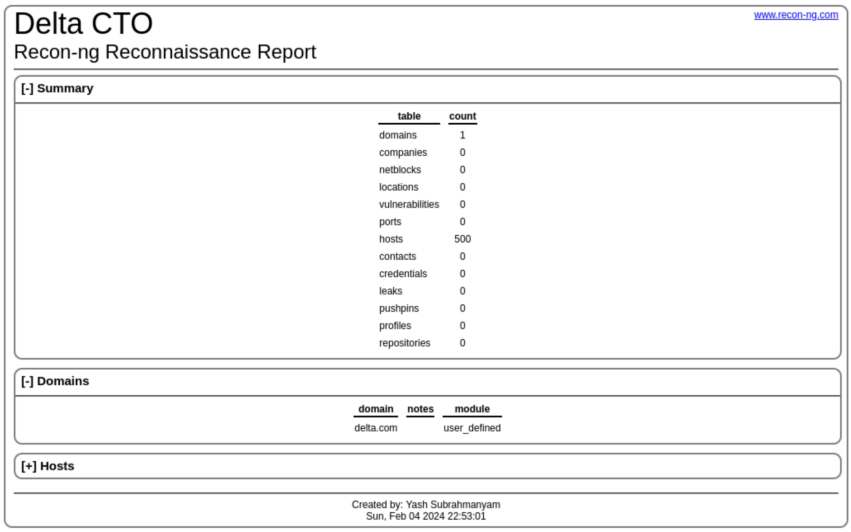
MXToolBox query:



SPF test using MXToolbox:



Recon-ng Reconnaissance report:



References

Convery-Pelletier, A. (2018, October 24). *The Delta Airlines Security Breach: A case study in how to respond to a data breach*. Radware Blog. https://www.radware.com/blog/security/2018/10/the-delta-airlines-security-breach-a-case-study-in-how-to-respond-to-a-data-breach/

Delta ESG Report 2021. delta.com. https://esghub.delta.com/information-security

Domain.com. (2021, March 12). *What is WHOIS and how is it used?: Domain.com: Blog*. domain.com . https://www.domain.com/blog/what-is-whois-and-how-is-it-used/

Nixintel. (2019, September 29). *Nixintel Open Source Intelligence & Investigations Getting started with Spiderfoot – a beginner's guide*. Nixintel Open Source Intelligence & Investigations. https://nixintel.info/osint-tools/getting-started-with-spiderfoot/