OLLSCOIL TEICNEOLAÍOCHTA
BHAILE ÁTHA CLIATH
DUBLIN
TECHNOLOGICAL
UNIVERSITY DUBLIN

Report

Assignment 1: Passive Reconnaissance Report

Company name: ReliaQuest

Student Name	Student Number	email address
Sebastian Konefal	**b00168561**	**b00168561@mytudublin.ie**

Digital Forensics and Cyber Security

TU765

Professional Penetration Testing DFCSH3014: 2024

Date: 10th November 2024

Table of Contents

1. Rules of Engagement and Scope

The Rules of Engagement for this passive reconnaissance project against ReliaQuest follow the best practices in FedRAMP Penetration Test Guidance. The scope is restricted explicitly to publicly available information. No active scanning, directly engaging with targets or exploitation attempts will be conducted. Only open-source intelligence (OSINT) tools and techniques shall be performed through DNS enumerations, web and database crawling, publicly accessible documents and social media profile analysis. The engagement will commence from 27 October 2024 to 20 November 2024, with weekly check-ins and progress reports to be submitted to John Johns, CISO in ReliaQuest (emergency contact 0896579776).

The pentesting team will consist of Sebastian Konefal LL.M, BA in Cybersecurity (pending), H.Dip. in Software Development (emergency contact 0894563445). All findings will be thoroughly documented, along with descriptions of any information gathered and possible implications to security.

The final report will summarise the passive reconnaissance activity, methodologies used, and recommendations. The report will then be encrypted via symmetric encryption AES-256 with a key previously agreed upon and safely exchanged with ReliaQuest, ensuring delivery confidentiality. The testing team will maintain confidentiality and handle all sensitive information in accordance with GDPR and ethical guidelines.

Any critical high-impact vulnerability identified shall immediately be brought to the notice of the CIO, CISO, and ISSO in line with requirements under NIST SP 800-115, Section 7. These guidelines ensure that the passive reconnaissance project aligns with the best practices of the FedRAMP Penetration Test Guidance and ensures a well-thought-out and compliant review of the ReliaQuest external footprint and related security risks.

2. Methodology

This report used a combination of passive reconnaissance and OSINT approach to identify vulnerabilities in the open-to-public infrastructure of ReliaQuest. Major steps included:

- The collection of information would be based on public sources such as DNS records, IP addresses, domain information and social media platforms. In this stage, no direct contact with the target assets was made, avoiding any potential risks of being detected.
- Mapping identified vulnerabilities to the MITRE ATT&CK framework in categorising potential attack vectors, including credential attacks, web application exploitation, DNS exposure, and cloud service misconfiguration.
- Documenting findings with recommendations on risk mitigations such as exposed employee data, login portals, cloud service configurations, publicly accessible DNS information.

The following work was proposed in a manner that was non-intrusive in an attempt to exhibit what may have been exposed by ReliaQuest without touching the integrity of the target environment in any way.

3. Company Background

ReliaQuest was founded by Brian Murphy, currently a CEO, in Tampa, Florida[1] in late 2007 and initially engaged in network engineering and IT including in the defence department. The company raised $300 million in funding led by the global investment firm, KKR and subsequently reached a valuation of over €1 billion in 2021[2]. The company provides cybersecurity services through its proprietary GrayMatter open XDR (extended detection and response) platform related to over 50 patents[3]. A press release published on 26th of September 2024 informed that the company launched an AI agent for security operations enhancing and automating threat detection, containment, investigation and response. In terms of the current company size, it has over 1,000 customers and 1,200 employees across six operation centres.[4]
The company participates in a vulnerability disclosure program in the Bugcrowd platform[5].

4. Information gathering

4.1.Company Website and Subdomains

The company operates as ReliaQuest, LLC with headquarters at Global Corporate Headquarters, 1001 Water St, Suite 1900 Tampa, FL 33602. The main website is located at: https://www.reliaquest.com/ with contact number of (800) 925-2159.

Example of the usual URL used:
https://www.reliaquest.com/resources/customer-stories/auto-club-group/

Example of URL providing a file:
https://www.reliaquest.com/wp-content/uploads/Security-Automation-Fundamentals-WP.pdf

Example of parameterized URL used:
https://www.reliaquest.com/news-and-press/page/3/?ft%5B0%5D=press-release&fd%5B0%5D=all

It appears that the company owns @reliaquest.com email domain as evidenced by further analysis and examples of info@reliaquest.com and employmentverifications@reliaquest.com or personal work email khill@reliaquest.com

Open positions under careers are seeking experience with Terraform, HelmDatadog, Prometheus, ActiveMQ, Kafka Snowflake, Splunk, QRadar, LogRhythm, Carbon Black, CrowdStrike, JS, Python, React, Angular, Typescript, Java, C#, AWS, Postgres, Apache Spark, Logstash, Hadoop/hive, Tensorflow, Kibana, Athena/Presto/BigTable, MySQL, Elasticsearch, SQL, Kubernetes (EKS), MSSQL, GitLab, Docker, GCP Azure Resource, Pods Litmos, Allego, Canvas, Blackboard.[6]

4.2.Press Release

- launched AI Agent, published in September 2024[7]

[1] https://venturebeat.com/security/reliaquest-maker-of-fast-growing-open-xdr-platform-reaches-1b-valuation/

[2] https://www.forbes.com/sites/karenwalker/2022/01/13/reliaquest-ceo-Con...-murphy-finds-success-with-hard-work-and-tailwinds/

[3] https://patents.justia.com/assignee/reliaquest-holdings-llc

[4] https://www.reliaquest.com/news-and-press/reliaquest-launches-first-autonomous-self-learning-ai-agent-for-security-operations/

[5] https://bugcrowd.com/engagements/reliaquest-vdpesf

[6] https://reliaquest.wd5.myworkdayjobs.com/ReliaQuest_Careers

[7] https://www.reliaquest.com/news-and-press/reliaquest-launches-first-autonomous-self-learning-ai-agent-for-security-operations/

- launched GreyMatter mobile app, lmorylak@reliaquest.com, published in March 2023[8]

- acquired agent software assets EclecticIQ, disclosed email address of r.benat@eclecticiq.com, khill@reliaquest.com, published in May 2023[9].

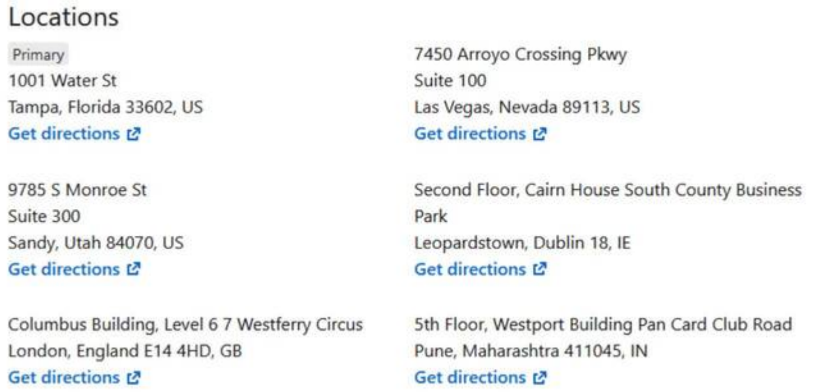
- launched Phishing Analyzer, published in March 2023[10].

- acquired Digital Shadows, published in June 2022[11]

- The company availed of PR services from Highwire PR (disclosed email addresses of reliaquest@highwirepr.com and press@reliaquest.com)[12]

4.3. LinkedIn

Locations of six operation centres:



Locations

Primary
1001 Water St
Tampa, Florida 33602, US
Get directions

7450 Arroyo Crossing Pkwy
Suite 100
Las Vegas, Nevada 89113, US
Get directions

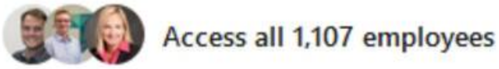
9785 S Monroe St
Suite 300
Sandy, Utah 84070, US
Get directions

Second Floor, Cairn House South County Business Park
Leopardstown, Dublin 18, IE
Get directions

Columbus Building, Level 6 7 Westferry Circus
London, England E14 4HD, GB
Get directions

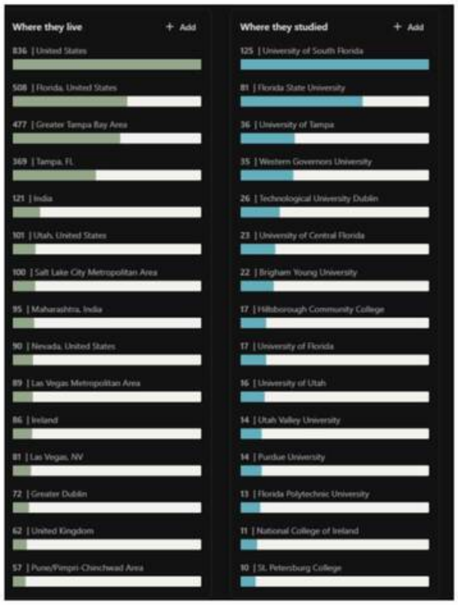
5th Floor, Westport Building Pan Card Club Road
Pune, Maharashtra 411045, IN
Get directions

Number of employees:



Access all 1,107 employees

Demography of employees:



[8] https://www.reliaquest.com/news-and-press/reliaquest-launches-greymatter-mobile-app/

[9] https://www.reliaquest.com/news-and-press/reliaquest-acquires-agent-software-and-engineering-assets-from-eclecticiq/

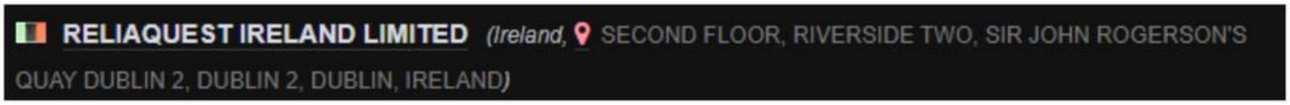
[10] https://www.reliaquest.com/news-and-press/reliaquest-launches-greymatter-phishing-analyzer/

[11] https://www.reliaquest.com/digital-shadows-acquisition/

[12] Ditto

4.4. Legal status of the company

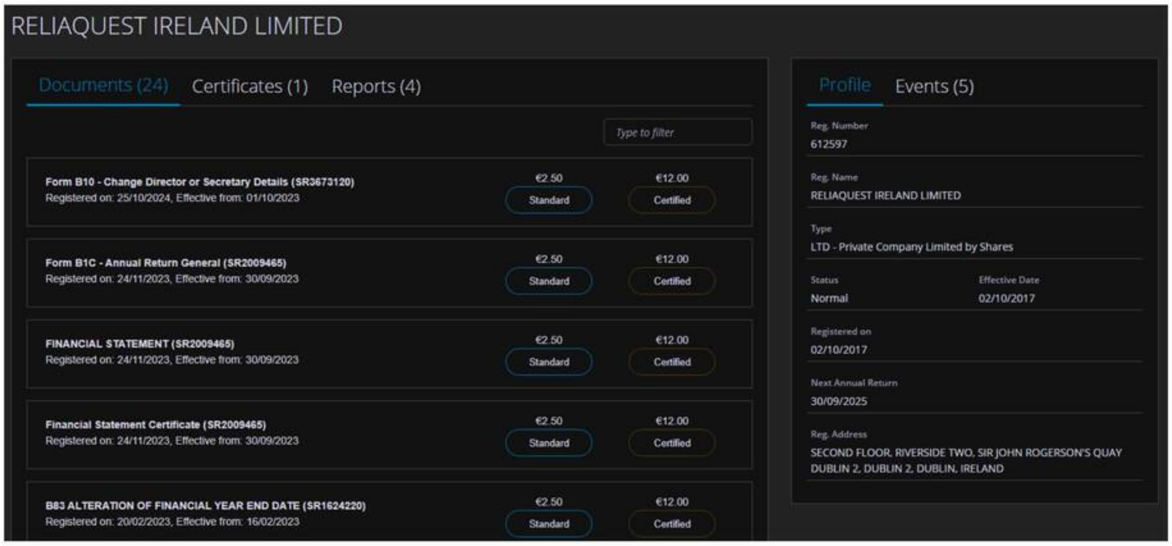
It was confirmed that ReliaQuest carries out its business in Ireland under Reliaquest Ireland Limited.



RELIAQUEST IRELAND LIMITED *(Ireland,* SECOND FLOOR, RIVERSIDE TWO, SIR JOHN ROGERSON'S QUAY DUBLIN 2, DUBLIN 2, DUBLIN, IRELAND*)*

Figure 1: https://opencorporates.com/companies?q=reliaquest&utf8=%E2%9C%93

Investigation in the Irish company register, run by the Department of Enterprise, Trade & Employment, confirms access to publicly available reports and financial statements.



RELIAQUEST IRELAND LIMITED

Form B10 - Change Director or Secretary Details (SR3673120) Registered on: 25/10/2024, Effective from: 01/10/2023	€2.50 Standard	€12.00 Certified
Form B1C - Annual Return General (SR2009465) Registered on: 24/11/2023, Effective from: 30/09/2023	€2.50 Standard	€12.00 Certified
FINANCIAL STATEMENT (SR2009465) Registered on: 24/11/2023, Effective from: 30/09/2023	€2.50 Standard	€12.00 Certified
Financial Statement Certificate (SR2009465) Registered on: 24/11/2023, Effective from: 30/09/2023	€2.50 Standard	€12.00 Certified
B83 ALTERATION OF FINANCIAL YEAR END DATE (SR1624220) Registered on: 20/02/2023, Effective from: 16/02/2023	€2.50 Standard	€12.00 Certified

Reg. Number
612597

Reg. Name
RELIAQUEST IRELAND LIMITED

Type
LTD - Private Company Limited by Shares

Status: Normal
Effective Date: 02/10/2017

Registered on
02/10/2017

Next Annual Return
30/09/2025

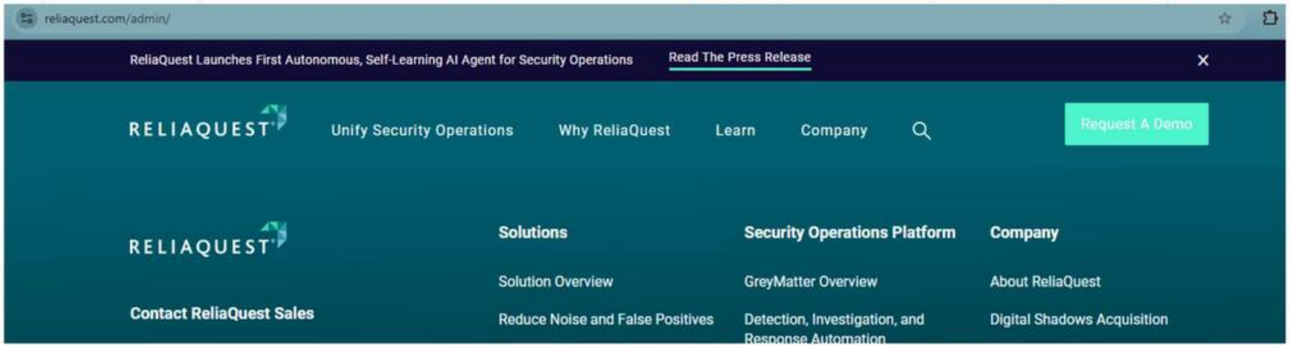
Reg. Address
SECOND FLOOR, RIVERSIDE TWO, SIR JOHN ROGERSON'S QUAY DUBLIN 2, DUBLIN 2, DUBLIN, IRELAND

Figure 2: https://core.cro.ie/e-commerce/company/645206

4.5. Google Dorking

Google Dorking is a technique to obtain search results by using advanced search queries/operators to obtain specific information unbiased by Google filters. The following queries were conducted revealing no potentially vulnerable information **expect for inurl:/admin/**:
site:reliaquest.com filetype:pdf, site:reliaquest.com filetype:docx, site:reliaquest.com filetype:ppt, site:reliaquest.com "internal use only", site:reliaquest.com "confidential", site:reliaquest.com intitle:"index of", site:reliaquest.com filetype:json, site:reliaquest.com filetype:env, site:reliaquest.com filetype:pdf "training", site:reliaquest.com inurl:login

quesry "site:reliaquest.com inurl:admin" returned URL: https://www.reliaquest.com/admin/ :



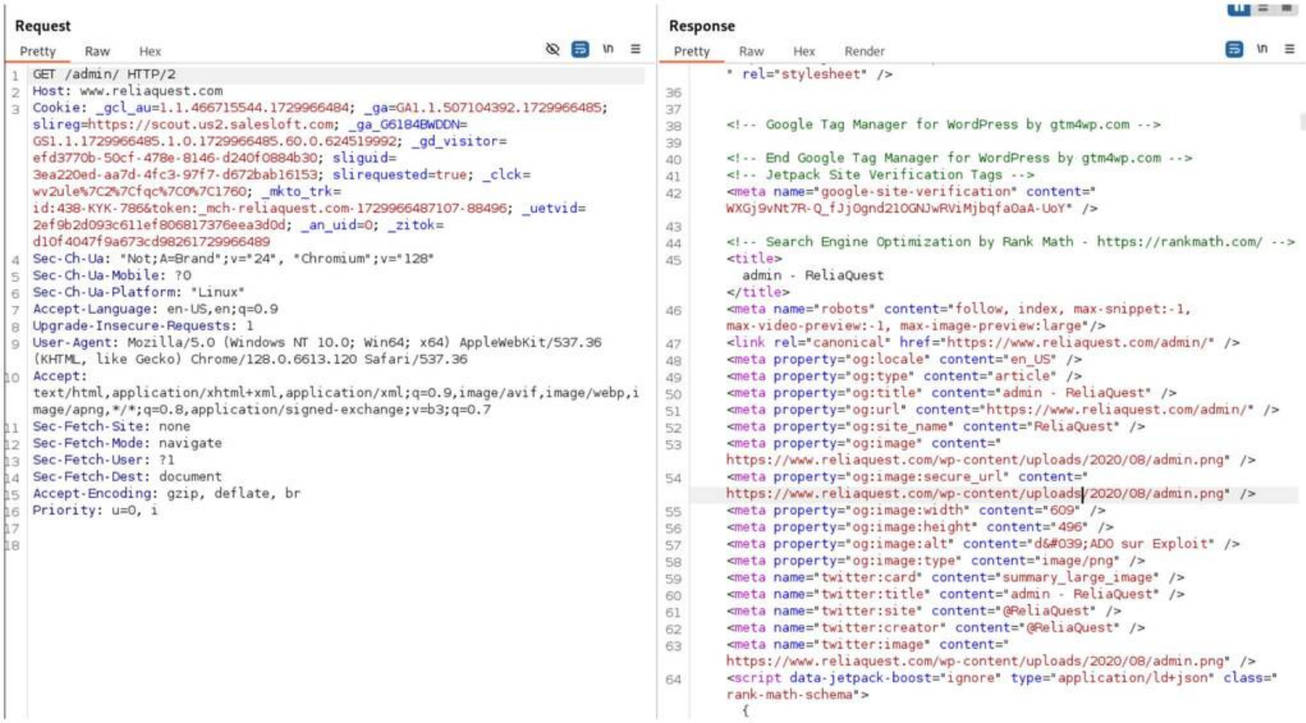
reliaquest.com/admin/

ReliaQuest Launches First Autonomous, Self-Learning AI Agent for Security Operations

Figure 3: https://www.reliaquest.com/admin/

Following the discovery of the admin page, the website was checked in BurpSuit for any interesting artefacts. The URL was found to contain a file named admin.png. Given that it was .png file that may contain scripts, before opening the file, it was checked with an Antivirus Clamscan and Exiftool for metadata that relieved the last modification on 31st August 2023. The file consisted of a **screenshot from Russian-language cybercrime forum exploit.im**. After translation, it was clear that the post was made in relation to user ADO and the resolution of a complaint.

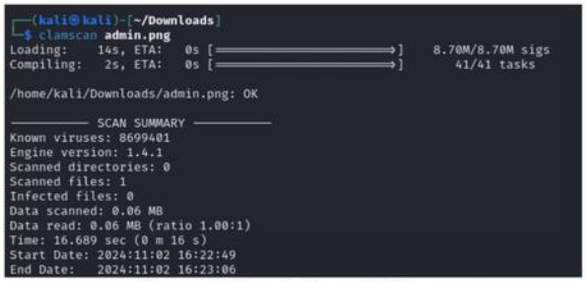
Given that the file is not rendered by the user's browser when assessing the website, there are only two possible explanations for the existence of this file. It might either be an artefact of a previously existing post related to the content of the screenshot or a honey file left by the company to monitor IP accessing /admin/ URL address.



```
GET /admin/ HTTP/2
Host: www.reliaquest.com
Cookie: _gcl_au=1.1.466715544.1729966484; _ga=GA1.1.507104392.1729966485;
slireg=https://scout.us2.salesloft.com; _ga_G6184BWDDN=
GS1.1.1729966485.1.0.1729966485.60.0.624519992; _gd_visitor=
efd3770b-50cf-478e-8146-d240f0884b30; sliguid=
3ea220ed-aa7d-4fc3-97f7-d672bab16153; slirequested=true; _clck=
wv2ule%7C2%7Cfqc%7C0%7C1760; _mkto_trk=
id:438-KYK-786&token:_mch-reliaquest.com-1729966487107-88496; _uetvid=
2ef9b2d093c611ef806817376eea3d0d; _an_uid=0; _zitok=
d10f4047f9a673cd98261729966489
Sec-Ch-Ua: "Not;A=Brand";v="24", "Chromium";v="128"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,i
mage/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

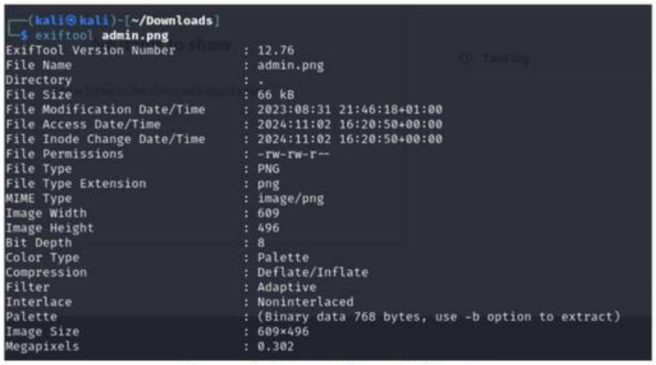
```
" rel="stylesheet" />


<!-- Google Tag Manager for WordPress by gtm4wp.com -->

<!-- End Google Tag Manager for WordPress by gtm4wp.com -->
<!-- Jetpack Site Verification Tags -->
<meta name="google-site-verification" content="
WXGj9vNt7R-Q_fJjOgnd21OGNJwRViMjbqfa0aA-UoY" />

<!-- Search Engine Optimization by Rank Math - https://rankmath.com/ -->
<title>
  admin - ReliaQuest
</title>
<meta name="robots" content="follow, index, max-snippet:-1,
max-video-preview:-1, max-image-preview:large"/>
<link rel="canonical" href="https://www.reliaquest.com/admin/" />
<meta property="og:locale" content="en_US" />
<meta property="og:type" content="article" />
<meta property="og:title" content="admin - ReliaQuest" />
<meta property="og:url" content="https://www.reliaquest.com/admin/" />
<meta property="og:site_name" content="ReliaQuest" />
<meta property="og:image" content="
https://www.reliaquest.com/wp-content/uploads/2020/08/admin.png" />
<meta property="og:image:secure_url" content="
https://www.reliaquest.com/wp-content/uploads/2020/08/admin.png" />
<meta property="og:image:width" content="609" />
<meta property="og:image:height" content="496" />
<meta property="og:image:alt" content="d&#039;ADO sur Exploit" />
<meta property="og:image:type" content="image/png" />
<meta name="twitter:card" content="summary_large_image" />
<meta name="twitter:title" content="admin - ReliaQuest" />
<meta name="twitter:site" content="@ReliaQuest" />
<meta name="twitter:creator" content="@ReliaQuest" />
<meta name="twitter:image" content="
https://www.reliaquest.com/wp-content/uploads/2020/08/admin.png" />
<script data-jetpack-boost="ignore" type="application/ld+json" class="
rank-math-schema">
  {
```

Figure 4: BurpSuit request and reply of https://www.reliaquest.com/admin/



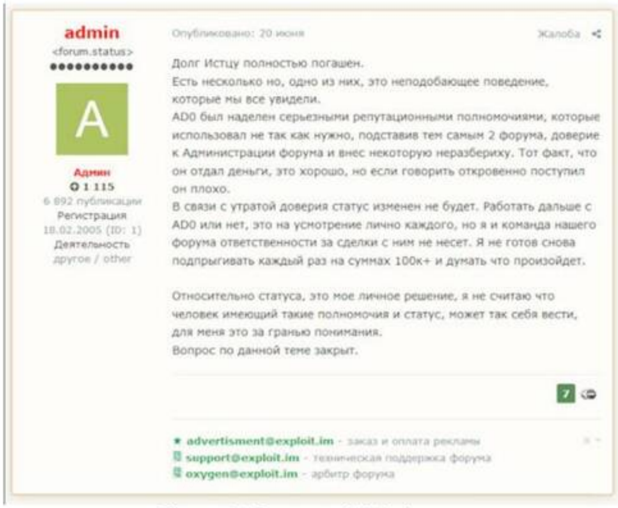
```
┌──(kali㉿kali)-[~/Downloads]
└─$ clamscan admin.png
Loading:    14s, ETA:   0s [========================>]    8.70M/8.70M sigs
Compiling:   2s, ETA:   0s [========================>]       41/41 tasks

/home/kali/Downloads/admin.png: OK

----------- SCAN SUMMARY -----------
Known viruses: 8699401
Engine version: 1.4.1
Scanned directories: 0
Scanned files: 1
Infected files: 0
Data scanned: 0.06 MB
Data read: 0.06 MB (ratio 1.00:1)
Time: 16.689 sec (0 m 16 s)
Start Date: 2024:11:02 16:22:49
End Date:   2024:11:02 16:23:06
```

Figure 5: Results from AV Clamscan



```
┌──(kali㉿kali)-[~/Downloads]
└─$ exiftool admin.png
ExifTool Version Number         : 12.76
File Name                       : admin.png
Directory                       : .
File Size                       : 66 kB
File Modification Date/Time     : 2023:08:31 21:46:18+01:00
File Access Date/Time           : 2024:11:02 16:20:50+00:00
File Inode Change Date/Time     : 2024:11:02 16:20:50+00:00
File Permissions                : -rw-rw-r--
File Type                       : PNG
File Type Extension             : png
MIME Type                       : image/png
Image Width                     : 609
Image Height                    : 496
Bit Depth                       : 8
Color Type                      : Palette
Compression                     : Deflate/Inflate
Filter                          : Adaptive
Interlace                       : Noninterlaced
Palette                         : (Binary data 768 bytes, use -b option to extract)
Image Size                      : 609×496
Megapixels                      : 0.302
```

Figure 6: Results from Exif tool



admin
<forum.status>

Админ
1 115
6 892 публикации
Регистрация
18.02.2005 (ID: 1)
Деятельность
другое / other

Опубликовано: 20 июня

Долг Истцу полностью погашен.
Есть несколько но, одно из них, это неподобающее поведение, которые мы все увидели.
AD0 был наделен серьезными репутационными полномочиями, которые использовал не так как нужно, подставив тем самым 2 форума, доверие к Администрации форума и внес некоторую неразбериху. Тот факт, что он отдал деньги, это хорошо, но если говорить откровенно поступил он плохо.
В связи с утратой доверия статус изменен не будет. Работать дальше с AD0 или нет, это на усмотрение лично каждого, но я и команда нашего форума ответственности за сделки с ним не несет. Я не готов снова подпрыгивать каждый раз на суммах 100к+ и думать что произойдет.

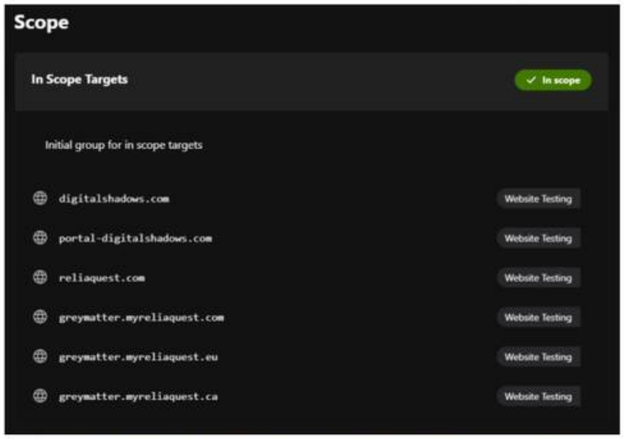
Относительно статуса, это мое личное решение, я не считаю что человек имеющий такие полномочия и статус, может так себя вести, для меня это за гранью понимания.
Вопрос по данной теме закрыт.

advertisment@exploit.im - заказ и оплата рекламы
support@exploit.im - техническая поддержка форума
oxygen@exploit.im - арбитр форума

Figure 7: Content of Admin.png

4.6.Vulnerability Disclosure Program

Participation in the Vulnerability Disclosure Program is a sign of a mature approach to cybersecurity wherein the company values feedback from white hat hackers, researchers and bug hunters to identify weaknesses. The program is powered by BugCrowd and there are two services available to log in, Digital Shadows and GreyMatter under this program.



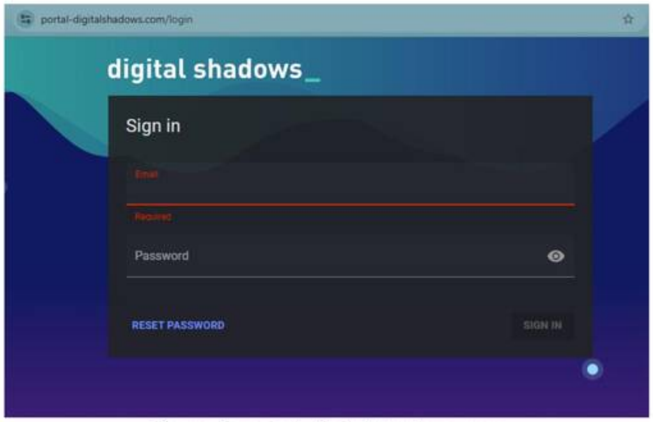
Scope

In Scope Targets ✓ In scope

Initial group for in scope targets

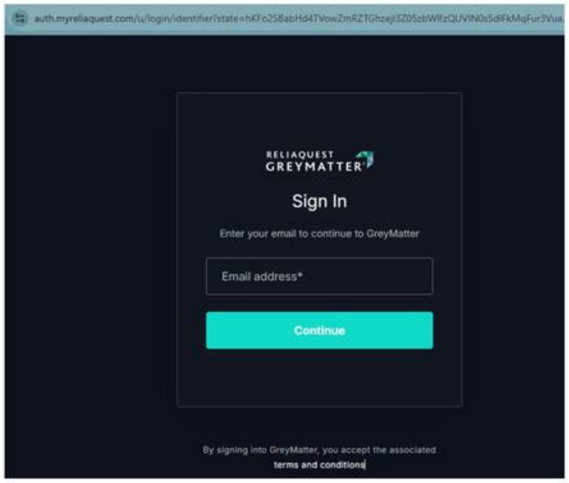
digitalshadows.com	Website Testing
portal-digitalshadows.com	Website Testing
reliaquest.com	Website Testing
greymatter.myreliaquest.com	Website Testing
greymatter.myreliaquest.eu	Website Testing
greymatter.myreliaquest.ca	Website Testing

Figure 8: https://bugcrowd.com/engagements/reliaquest-vdpesf



portal-digitalshadows.com/login

Figure 9: portal-digitalshadows.com



auth.myreliaquest.com/u/login/identifier?state=hKFo2SBabHd4TVowZmRZTGhzejl3Z05zbWRzQUVlN0s5dlFkMqFur3Vua

RELIAQUEST GREYMATTER
Sign In
Enter your email to continue to GreyMatter
Email address*
Continue
By signing into GreyMatter, you accept the associated terms and conditions

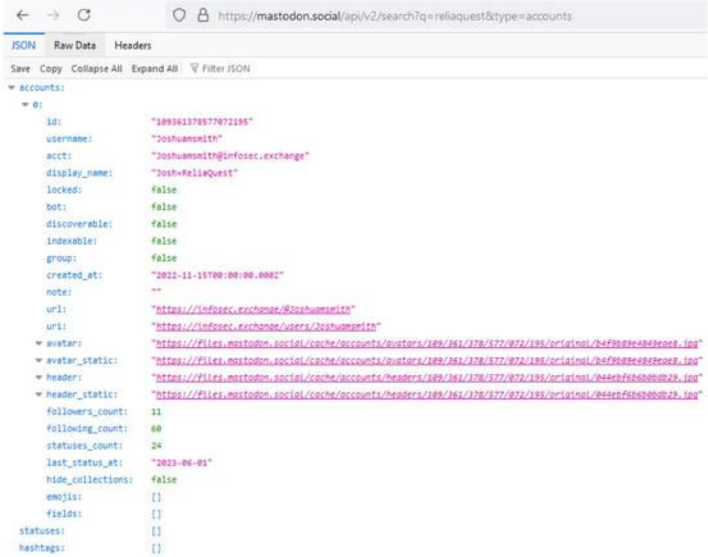
Figure 10: greymatter.myreliaquest.com

5. Technical Footprint

5.1.whatsmyname.app

https://whatsmyname.app/ is a web-based tool that allows the user to perform username search across multiple websites, platforms and social media websites. A search of phrase "ReliaQuest" was performed against 600 websites and the most notable results consisted of:

- JSON API details to Mastodon (social media website) created in 2022 and containing the email address Joshuamsmith@infosec.exchange

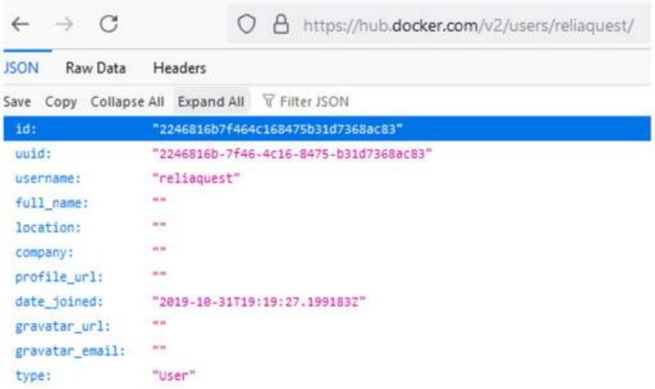


https://mastodon.social/api/v2/search?q=reliaquest&type=accounts
JSON
Raw Data
Headers
Save
Copy
Collapse All
Expand All
Filter JSON

```
▾ accounts:
  ▾ 0:
      id:                "109361378577072195"
      username:          "Joshuamsmith"
      acct:              "Joshuamsmith@infosec.exchange"
      display_name:      "Josh+ReliaQuest"
      locked:            false
      bot:               false
      discoverable:      false
      indexable:         false
      group:             false
      created_at:        "2022-11-15T00:00:00.000Z"
      note:              ""
      url:               "https://infosec.exchange/@Joshuamsmith"
      uri:               "https://infosec.exchange/users/Joshuamsmith"
    ▾ avatar:            "https://files.mastodon.social/cache/accounts/avatars/109/361/378/577/072/195/original/b4f9b89e4849ede8.jpg"
    ▾ avatar_static:     "https://files.mastodon.social/cache/accounts/avatars/109/361/378/577/072/195/original/b4f9b89e4849ede8.jpg"
    ▾ header:            "https://files.mastodon.social/cache/accounts/headers/109/361/378/577/072/195/original/044ebf6b6b0bdb29.jpg"
    ▾ header_static:     "https://files.mastodon.social/cache/accounts/headers/109/361/378/577/072/195/original/044ebf6b6b0bdb29.jpg"
      followers_count:   11
      following_count:   60
      statuses_count:    24
      last_status_at:    "2023-06-01"
      hide_collections:  false
      emojis:            []
      fields:            []
  statuses:              []
  hashtags:              []
```

Figure 11: https://mastodon.social/api/v2/search?q=reliaquest&type=accounts

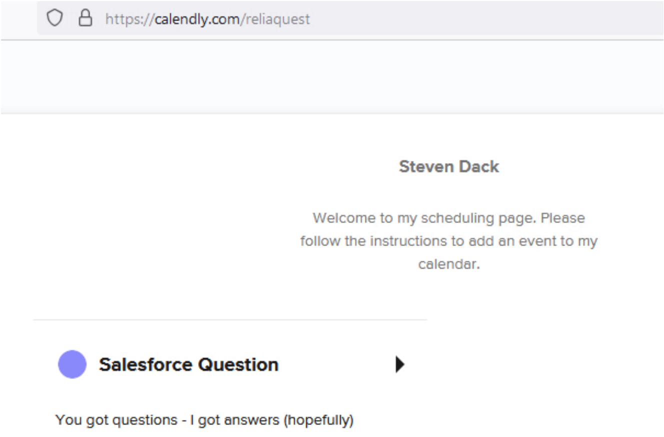
- JSON details to user profile from Docker Hub



```
id:              "2246816b7f464c168475b31d7368ac83"
uuid:            "2246816b-7f46-4c16-8475-b31d7368ac83"
username:        "reliaquest"
full_name:       ""
location:        ""
company:         ""
profile_url:     ""
date_joined:     "2019-10-31T19:19:27.199183Z"
gravatar_url:    ""
gravatar_email:  ""
type:            "User"
```

Figure 12: https://hub.docker.com/v2/users/reliaquest/

- Meeting scheduling page created by Calendly to book appointments with Steven Dack - Senior CRM Systems Architect – ReliaQuest. The application initially loads a calendar and instantly redirects and reloads the page informing that "This calendar is currently unavailable". This indicated that there might be room for exploitation


https://calendly.com/reliaquest

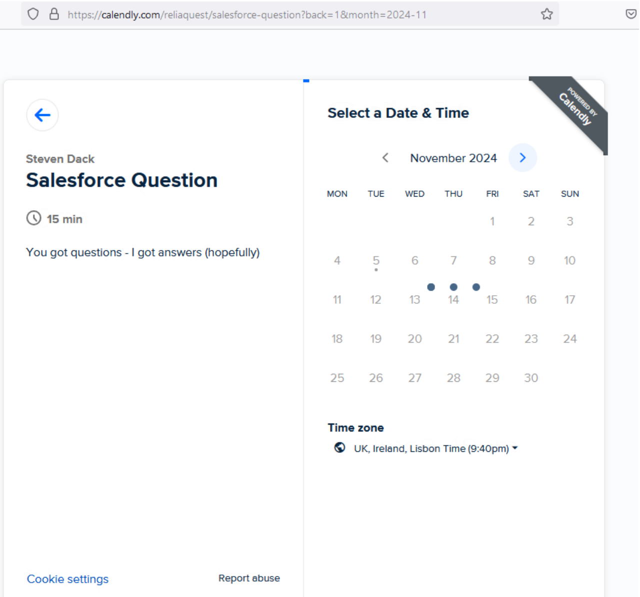
Steven Dack

Welcome to my scheduling page. Please follow the instructions to add an event to my calendar.

Salesforce Question

You got questions - I got answers (hopefully)

Figure 13: https://calendly.com/reliaquest


https://calendly.com/reliaquest/salesforce-question?back=1&month=2024-11

Steven Dack

Salesforce Question

15 min

You got questions - I got answers (hopefully)

Select a Date & Time

November 2024

MON	TUE	WED	THU	FRI	SAT	SUN
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

Time zone

UK, Ireland, Lisbon Time (9:40pm)

Cookie settings

Report abuse

Figure 14: https://calendly.com/reliaquest

- https://Confidential/ReliaQuest is followed by Confidential as per his LinkedIn account https://www.linkedin.com/in/Confidential profile, under the nickname Confidential https://Confidential and his GitHub profile https://github.com/Confidential confirm his personal email address: Confidential This email is not available on his LinkedIn profile. Further investigation at https://haveibeenpwned.com/ proves that this Gmail account was found in **37 data breaches**, last in September 2024. This information can be used in the subsequent steps of the penetration test by obtaining hashes of the passwords and attempting to use password-cracking techniques such as dictionary attacks using Jonh the Ripper, Hashcar or Hydra. Another option would be to perform a watering hole attack against the platforms that the subject might still be using. In this case, the subject was involved in the famous ParkMobile data breach in 2021 where email addresses, licence plates, names, passwords, and phone numbers were made available. Information from this breach enables us to find out through third-party services the subject's car make, and model but most importantly, the subject's place of residence. The findings could be further enhanced and investigated from the data involved in The Post Millennial from May 2024 and other breaches where subject's email addresses, genders, names, passwords, physical addresses, usernames, dates of birth, private messages, phone numbers, IP addresses, geographic locations, partial credit card data, device information, encrypted keys, website activity phone number were disclosed. Further investigation of the direct analysis of the data from the data breaches might be considered.

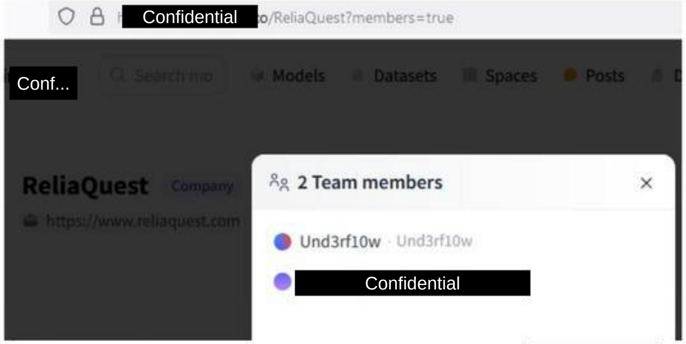


Figure 15: Team members following ReliaQuest in Confidential *https:/* Confidential */ReliaQuest*

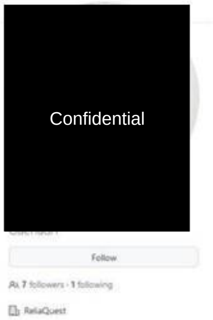
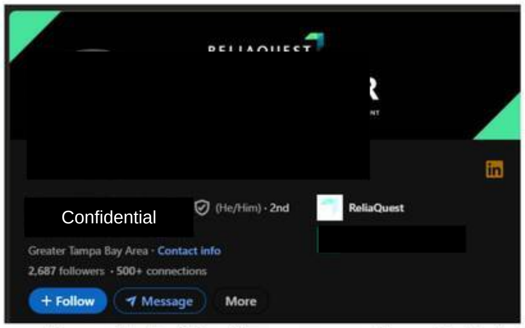
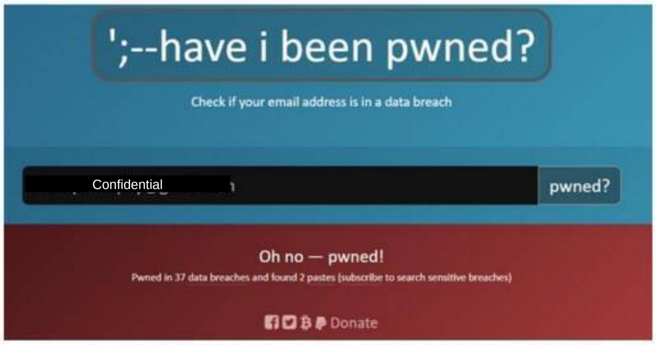


Figure 16: Profile of Confidential *y from GitHub https://github.com/* Confidential



RELIAQUEST
Confidential
(He/Him) · 2nd
ReliaQuest
Greater Tampa Bay Area · Contact info
2,687 followers · 500+ connections
+ Follow
Message
More

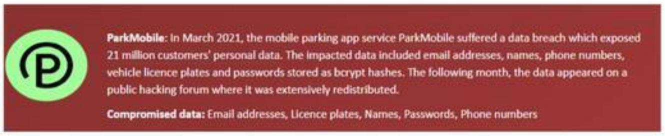
Figure 17: Profile of Confidential *from his LinkedIn account*



Oh no — pwned!

Pwned in 37 data breaches and found 2 pastes (subscribe to search sensitive breaches)

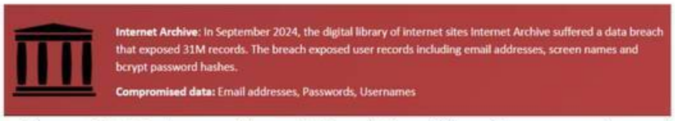
Figure 18: Results from https://haveibeenpwned.com



ParkMobile: In March 2021, the mobile parking app service ParkMobile suffered a data breach which exposed 21 million customers' personal data. The impacted data included email addresses, names, phone numbers, vehicle licence plates and passwords stored as bcrypt hashes. The following month, the data appeared on a public hacking forum where it was extensively redistributed.

Compromised data: Email addresses, Licence plates, Names, Passwords, Phone numbers

Figure 19: ParkMobile breach from https://haveibeenpwned.com/

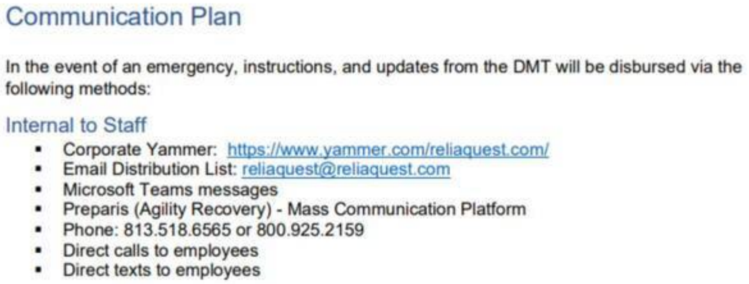


Internet Archive: In September 2024, the digital library of internet sites Internet Archive suffered a data breach that exposed 31M records. The breach exposed user records including email addresses, screen names and bcrypt password hashes.

Compromised data: Email addresses, Passwords, Usernames

Figure 20: Most recent breach from https://haveibeenpwned.com/

- Agency Term Contract for Security Operations Platform with State of Florida 2023, page 47 consists of ReliaQuest Security Operations Platform Solution and page 68 reveals usage of https://www.yammer.com/reliaquest.com/ and email address reliaquest@reliaquest.com



Communication Plan

In the event of an emergency, instructions, and updates from the DMT will be disbursed via the following methods:

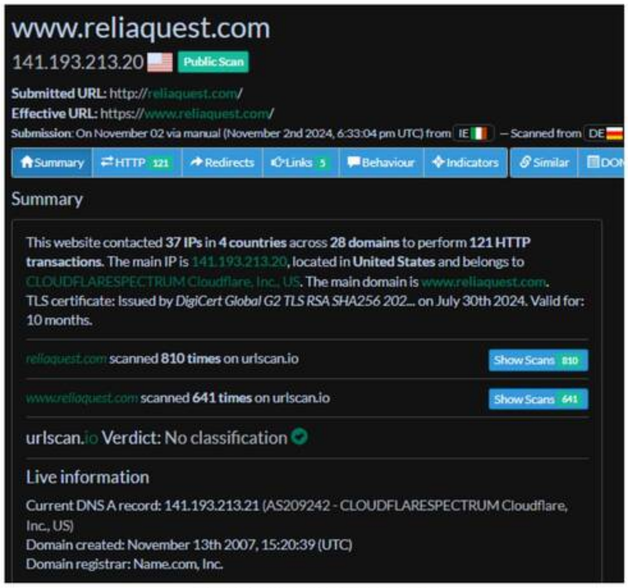
Internal to Staff

- Corporate Yammer: https://www.yammer.com/reliaquest.com/
- Email Distribution List: reliaquest@reliaquest.com
- Microsoft Teams messages
- Preparis (Agility Recovery) - Mass Communication Platform
- Phone: 813.518.6565 or 800.925.2159
- Direct calls to employees
- Direct texts to employees

Figure 21: https://cybergrants.fl.gov/download/agency_term_contracts/DMS-2223-157CSecurityOperationsPlatform-Insight-ReliaQuest/DMS-2223-157C-ATC-Final.pdf

5.2.urlscan.io

urlscan.io is a web-based tool that performs a scan of a given website. It confirmed the main IP address as 141.193.213.20 and DNS A record 141.193.213.21 issued by Cloudflare Spectrum, Cloudflare, Inc., United States (AS209242), TLS certificate issued by DigiCert Global G2 TLS RSA SHA256 valid for 10 months, and domain registrar as Name.com, Inc. created on the 13th of November 2007.



www.reliaquest.com

141.193.213.20 Public Scan

Submitted URL: http://reliaquest.com/

Effective URL: https://www.reliaquest.com/

Submission: On November 02 via manual (November 2nd 2024, 6:33:04 pm UTC) from IE — Scanned from DE

Summary

This website contacted **37 IPs** in **4 countries** across **28 domains** to perform **121 HTTP transactions.** The main IP is 141.193.213.20, located in **United States** and belongs to CLOUDFLARESPECTRUM Cloudflare, Inc., US. The main domain is www.reliaquest.com. TLS certificate: Issued by *DigiCert Global G2 TLS RSA SHA256 202...* on July 30th 2024. Valid for: 10 months.

reliaquest.com scanned **810 times** on urlscan.io — Show Scans 810

www.reliaquest.com scanned **641 times** on urlscan.io — Show Scans 641

urlscan.io Verdict: No classification

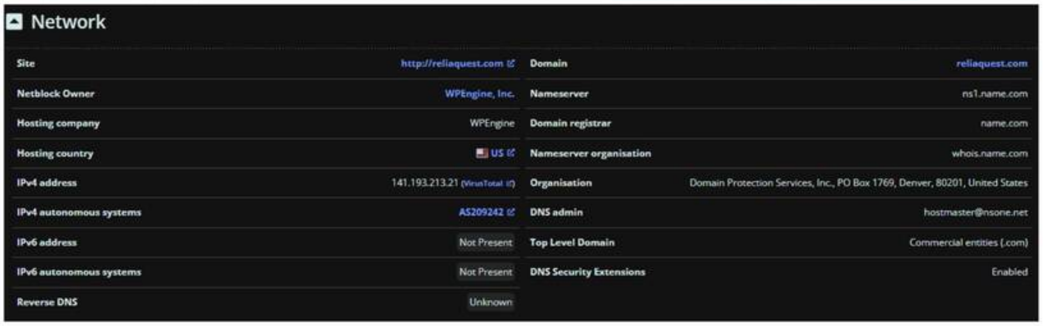
Live information

Current DNS A record: 141.193.213.21 (AS209242 - CLOUDFLARESPECTRUM Cloudflare, Inc., US)
Domain created: November 13th 2007, 15:20:39 (UTC)
Domain registrar: Name.com, Inc.

Figure 22: urlscan.io scan

5.3.Netcraft

Netcraft is an online tool and service that shows information about a website's infrastructure. The network owner, WPEngine, Inc. and contact to DNS admin hostmaster@nsone.net were obtained.[13]



Network

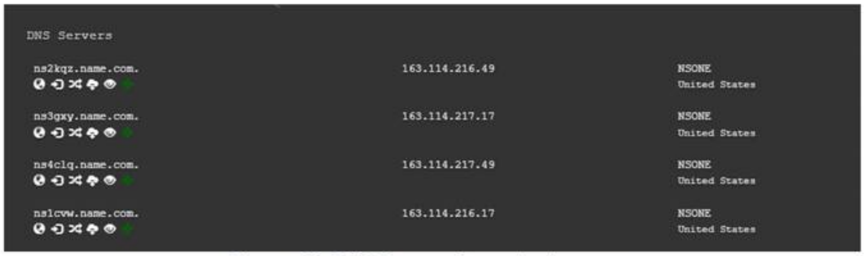
Site	http://reliaquest.com	**Domain**	reliaquest.com
Netblock Owner	WPEngine, Inc.	**Nameserver**	ns1.name.com
Hosting company	WPEngine	**Domain registrar**	name.com
Hosting country	US	**Nameserver organisation**	whois.name.com
IPv4 address	141.193.213.21 (VirusTotal)	**Organisation**	Domain Protection Services, Inc., PO Box 1769, Denver, 80201, United States
IPv4 autonomous systems	AS209242	**DNS admin**	hostmaster@nsone.net
IPv6 address	Not Present	**Top Level Domain**	Commercial entities (.com)
IPv6 autonomous systems	Not Present	**DNS Security Extensions**	Enabled
Reverse DNS	Unknown		

Figure 23: Netcraft result

5.4.dnsdumpster

https://dnsdumpster.com/ -

In addition to the IPs of the DNS servers, the results confirmed DNS Hosting Provider as: Name.com with NSONE service (traffic management service) and list of subdomains and VPN endpoints.

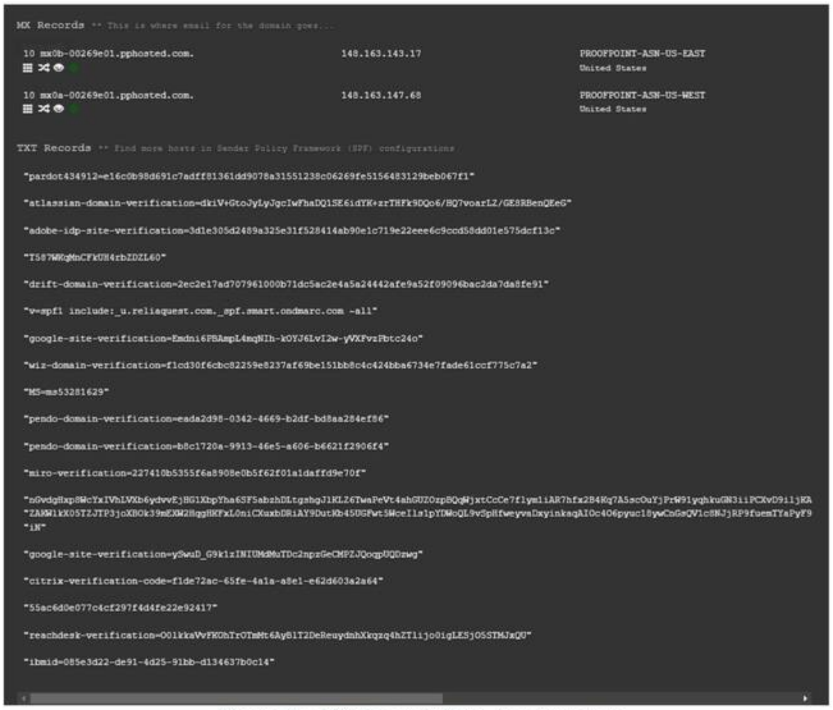


```
DNS Servers

 ns2kqz.name.com.            163.114.216.49         NSONE
                                                    United States
 ns3gxy.name.com.            163.114.217.17         NSONE
                                                    United States
 ns4clq.name.com.            163.114.217.49         NSONE
                                                    United States
 ns1cvw.name.com.            163.114.216.17         NSONE
                                                    United States
```

Figure 24: DNS Servers from dnsdumpster

[13] https://sitereport.netcraft.com/?url=http://reliaquest.com

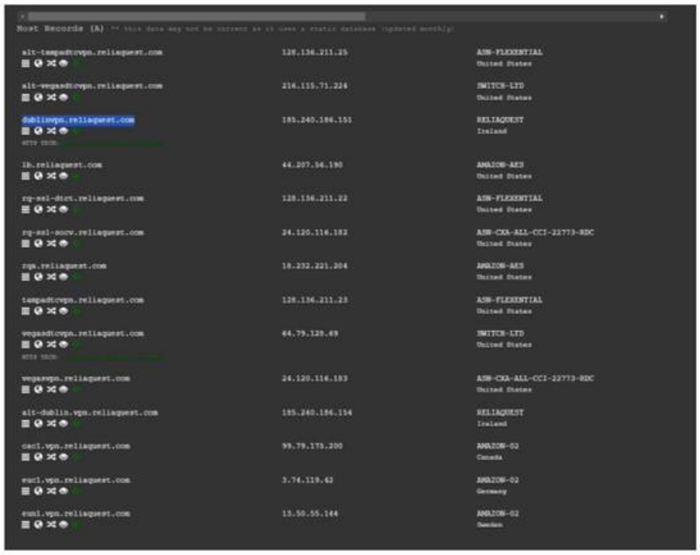
It is worth noting from the MX records that mail is being sent to Proofpoint system and potential phishing emails should be capable of avoiding Proofpoint phasing filtering system. TXT records include SPF configuration and third-party service unique verification tokens (IMB, Microsoft, Google, Adobe etc.). **No DMARC or DKIM.**



```
MX Records ** This is where email for the domain goes...

 10 mx0b-00269e01.pphosted.com.        148.163.143.17        PROOFPOINT-ASN-US-EAST
                                                             United States
 10 mx0a-00269e01.pphosted.com.        148.163.147.68        PROOFPOINT-ASN-US-WEST
                                                             United States

TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations

 "pardot434912=e16c0b98d691c7adff81361dd9078a31551238c06269fe5156483129beb067f1"

 "atlassian-domain-verification=dkiV+GtoJyLyJgcIwFhaDQ1SE6idYK+zrTHFk9DQo6/BQ7voarLZ/GE8RBenQEeG"

 "adobe-idp-site-verification=3d1e305d2489a325e31f528414ab90e1c719e22eee6c9ccd58dd01e575dcf13c"

 "TS87WKgMnCFkUH4rbZDZL60"

 "drift-domain-verification=2ec2e17ad707961000b71dc5ac2e4a5a24442afe9a52f09096bac2da7da8fe91"

 "v=spf1 include:_u.reliaquest.com._spf.smart.ondmarc.com -all"

 "google-site-verification=Emdni6PBAmpL4mqNIh-kOYJ6LvI2w-yVXFvzFbtc24o"

 "wiz-domain-verification=f1cd30f6cbc82259e8237af69be151bb8c4c424bba6734e7fade61ccf775c7a2"

 "MS=ms53281629"

 "pendo-domain-verification=eada2d98-0342-4669-b2df-bd8aa284ef86"

 "pendo-domain-verification=b8c1720a-9913-46e5-a606-b6621f2906f4"

 "miro-verification=227410b5355f6a8908e0b5f62f01a1daffd9e70f"

 "nGvdgHxp8WcYxIVhLVXb6ydvvEjHG1XbpYha6SF5abzhDLtgshgJ1KLZ6TwaPeVt4ahGUZ0zpBQqWjxtCcCe7f1ym1iAR7hfx2B4Kq7A5scOuYjPrW91yqhkuGN3iiPCXvD9i1jKA
 "ZAKW1kX05TZJTP3joXBOk39mEXW2HqgHKFxL0niCXuxbDRiAY9DutKb45UGFwt5WceIls1pYDWoQL9vSpHfweyvaDxyinkaqAIOc406pyuc18ywCnGsQV1c8NJjRP9fuemTYaPyF9
 "iN"

 "google-site-verification=ySwuD_G9k1zINIUMdMuTDc2npzGeCMPZJQoqpUQDzwg"

 "citrix-verification-code=f1de72ac-65fe-4a1a-a8e1-e62d603a2a64"

 "55ac6d0e077c4cf297f4d4fe22e92417"

 "reachdesk-verification=O01kkaVvFKOhTrOTmMt6AyB1T2DeReuydnhXkqzq4hZT1ijo0igLESjOSSTMJxQU"

 "ibmid=085e3d22-de91-4d25-91bb-d134637b0c14"
```

Figure 25: MX Records from dnsdumpster

All of the Host IP records provide a list of IP A Records related to specific services such as VPNs and load balancers. None of the addresses are safely operational via the browser and an error for unsecure connection is displayed net::ERR_CERT_AUTHORITY_INVALID. AWS, Flexential and Switch were revealed as hosting providers



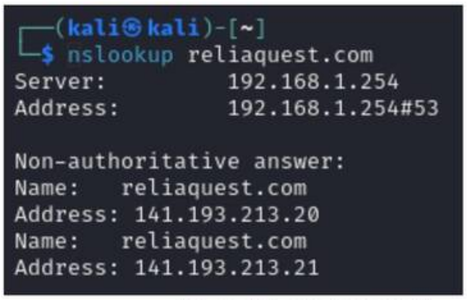
```
Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

 alt-tampadtcvpn.reliaquest.com       128.136.211.25       ASN-FLEXENTIAL
                                                           United States
 alt-vegasdtcvpn.reliaquest.com       216.115.71.224       SWITCH-LTD
                                                           United States
 dublinvpn.reliaquest.com             185.240.186.151      RELIAQUEST
                                                           Ireland
 lb.reliaquest.com                    44.207.56.190        AMAZON-AES
                                                           United States
 rq-ssl-dtct.reliaquest.com           128.136.211.22       ASN-FLEXENTIAL
                                                           United States
 rq-ssl-socv.reliaquest.com           24.120.116.182       ASN-CXA-ALL-CCI-22773-RDC
                                                           United States
 rqs.reliaquest.com                   18.232.221.204       AMAZON-AES
                                                           United States
 tampadtcvpn.reliaquest.com           128.136.211.23       ASN-FLEXENTIAL
                                                           United States
 vegasdtcvpn.reliaquest.com           64.79.128.69         SWITCH-LTD
                                                           United States
 vegasvpn.reliaquest.com              24.120.116.183       ASN-CXA-ALL-CCI-22773-RDC
                                                           United States
 alt-dublin.vpn.reliaquest.com        185.240.186.154      RELIAQUEST
                                                           Ireland
 cac1.vpn.reliaquest.com              99.79.175.200        AMAZON-02
                                                           Canada
 euc1.vpn.reliaquest.com              3.74.119.62          AMAZON-02
                                                           Germany
 eun1.vpn.reliaquest.com              13.50.55.144         AMAZON-02
                                                           Sweden
```

Figure 26: Host Records

5.5.Nslookup and Whois

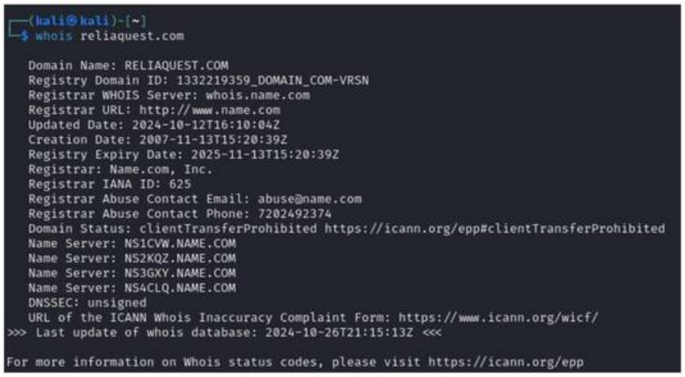
Nslookup revealed that there are two IP addresses, implying that there might be a firewall:

Extract from whois command that confirmed URL registrar, certificate expiry and **DNSSEC unsigned**:



```
┌──(kali㉿kali)-[~]
└─$ nslookup reliaquest.com
Server:         192.168.1.254
Address:        192.168.1.254#53

Non-authoritative answer:
Name:   reliaquest.com
Address: 141.193.213.20
Name:   reliaquest.com
Address: 141.193.213.21
```

Figure 27: nslookup result

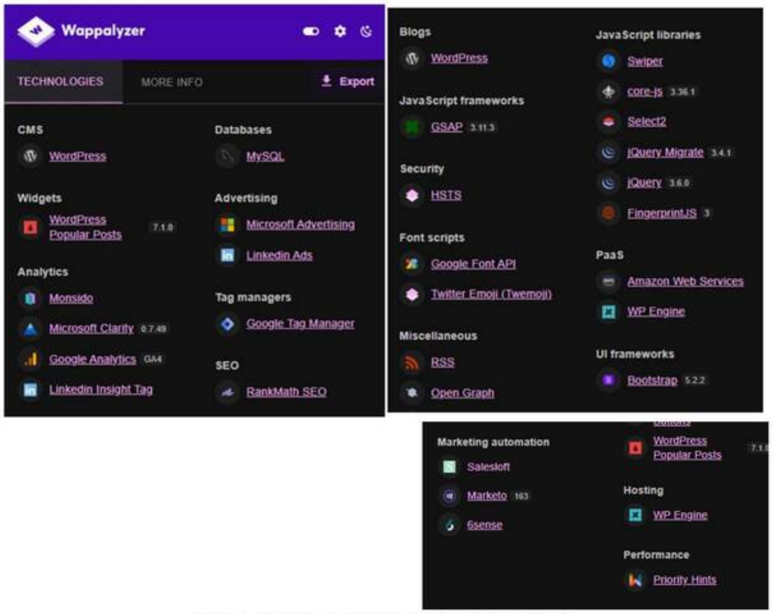


```
┌──(kali㉿kali)-[~]
└─$ whois reliaquest.com

   Domain Name: RELIAQUEST.COM
   Registry Domain ID: 1332219359_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.name.com
   Registrar URL: http://www.name.com
   Updated Date: 2024-10-12T16:10:04Z
   Creation Date: 2007-11-13T15:20:39Z
   Registry Expiry Date: 2025-11-13T15:20:39Z
   Registrar: Name.com, Inc.
   Registrar IANA ID: 625
   Registrar Abuse Contact Email: abuse@name.com
   Registrar Abuse Contact Phone: 7202492374
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Name Server: NS1CVW.NAME.COM
   Name Server: NS2KQZ.NAME.COM
   Name Server: NS3GXY.NAME.COM
   Name Server: NS4CLQ.NAME.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-10-26T21:15:13Z <<<

For more information on Whois status codes, please visit https://icann.org/epp
```

Figure 28: whois result

5.6.Identified Technology Stack

Wappalyzer browser extension provided that WordPress is used as a Content Management System and WordPress Popular Posts (version 7.10 – most up-to-date version), WP Engine and Amazon CDN were used as content delivery networks, jQuery 3.6.0 and GSAP, core-js 3.36.1 JavaScript libraries were used, Bootstrap 5.2 and Swiper were used for user interface and FingerprintJS indicates user tracking mechanism. Finally, security headers indicate the usage of HTTP/3. **There is no version of used WordPress** provided and the website lacks the tag of meta name="generator" content= "WordPress ..." to investigate the version.



CMS
WordPress

Widgets
WordPress Popular Posts 7.1.0

Analytics
Monsido
Microsoft Clarity 0.7.49
Google Analytics GA4
Linkedin Insight Tag

Databases
MySQL

Advertising
Microsoft Advertising
Linkedin Ads

Tag managers
Google Tag Manager

SEO
RankMath SEO

Blogs
WordPress

JavaScript frameworks
GSAP 3.11.3

Security
HSTS

Font scripts
Google Font API
Twitter Emoji (Twemoji)

Miscellaneous
RSS
Open Graph

JavaScript libraries
Swiper
core-js 3.36.1
Select2
jQuery Migrate 3.4.1
jQuery 3.6.0
FingerprintJS 3

PaaS
Amazon Web Services
WP Engine

UI frameworks
Bootstrap 5.2.2

PyScript
HTTP/3

Programming languages
Python
PHP

CDN
jsDelivr
jQuery CDN
cdnjs
Cloudflare
Amazon S3

Marketing automation

Monsido

Accessibility
Monsido

Personalisation
6sense

Browser fingerprinting
FingerprintJS 3

WordPress plugins
RankMath SEO
SVG Support
AddToAny Share Buttons
WordPress

Marketing automation
Salesloft
Marketo 163
6sense

WordPress Popular Posts 7.1.0

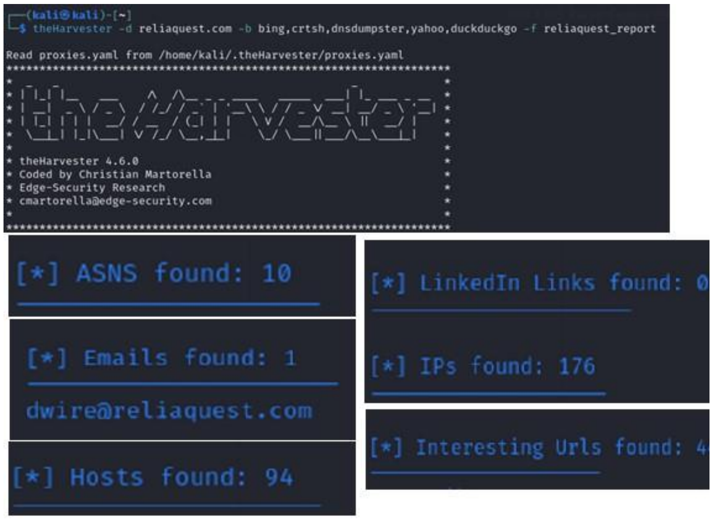
Hosting
WP Engine

Performance
Priority Hints

Figure 29 Wappalyzer technology stack

5.7.theHarvester

theHarvester is a gathering tool that obtains information from multiple public sources such as bing, crtsh, dnsdumpster and many others, however some sources require API keys. Google is no longer included in the sources. The version of theHarvester used was 4.6.0 and the following command was run: "*theHarvester -d reliaquest.com -b all -l 200 -f reliaquest_report*" which revealed one email address dwire@reliaquest.com, 94 Hosts, 176 IPs, 10 Autonomous System Number (ASNS) used in Border Gateway Protocol routing, and 44 interesting URLs. Due to the size of the information, please see Appendix 1 to obtain the full results.



```
┌──(kali㉿kali)-[~]
└─$ theHarvester -d reliaquest.com -b bing,crtsh,dnsdumpster,yahoo,duckduckgo -f reliaquest_report

Read proxies.yaml from /home/kali/.theHarvester/proxies.yaml
*******************************************************************
*                                                                 *
* theHarvester 4.6.0                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************
```

```
[*] ASNS found: 10
```

```
[*] Emails found: 1

dwire@reliaquest.com
```

```
[*] Hosts found: 94
```

```
[*] LinkedIn Links found: 0
```

```
[*] IPs found: 176
```

```
[*] Interesting Urls found: 4
```

Figure 30: Results from the Harvester

Summary of interesting hosts:

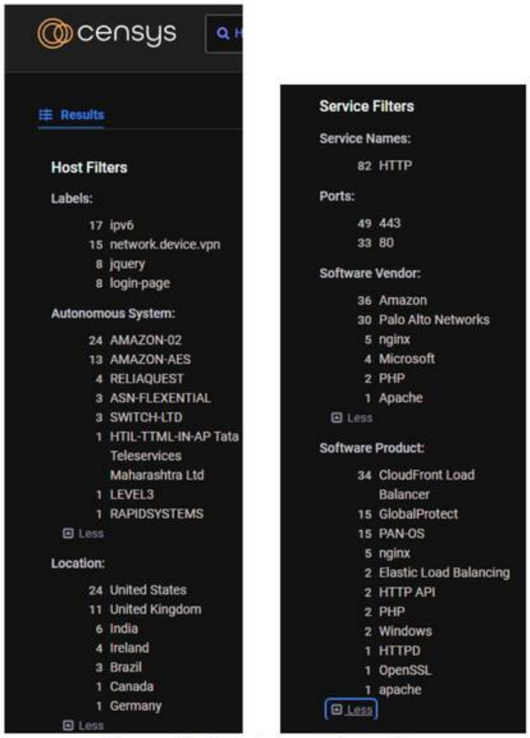
• Microsoft Exchange's Autodiscover service	autodiscover.reliaquest.com, agentvpn.reliaquest.com
• Likely a central access	portal.reliaquest.com
• Potentially associated with security intelligence or threat intelligence services	security.reliaquest.com and intel.reliaquest.com
• Multiple VPN hosts	tampadtcvpn.reliaquest.com,vegasdtcvpn.reliaquest.com , and alt-dublin.vpn.reliaquest.com
• mail server potentially exposing email protocols	mail.reliaquest.com
• webmail access point	webmail.reliaquest.com

Summary of Interesting URLs:

This appears to be a primary host used for tracking URLs and loading images in emails; thus, it might be part of company marketing and tracking efforts - likely Marketo already discovered.	https://email.reliaquest.com
This host includes links related to preference management and hosted images for email content. It looks like a gateway to the content and the interaction of forms. Such pages might show user touchpoints and subscription management features that can be quite insightful in understanding user journeys of engagement.	https://go.reliaquest.com
Although this URL was listed only once, it may be considered a part of some specialised service or log-in portal. It could most likely be associated with a subdomain used for one of the product or service lines and could be useful upon deeper searches, whether leading to secure or restricted-access content.	https://sl.reliaquest.com

5.8. Censys

Censys is a web-based tool that actively scan the online resources and organises this information into a searchable database. The search against reliaquest.com confirmed the presence of IPv6, VPNs, jquesty and login-pages. In terms of the infrastructure, the report provided that the majority of traffic is routed via AMAZON-02, AMAZON-AES and connected to ReliaQuest (RELIAQUEST), and confirmed previous findings of Flexential and Switch ASN. Most servers are located in the United States and United Kingdom with some presence in India, Ireland, Brazil, Canada and Germany. The only services available on the hosts are limited to port 80 - HTTP and 443 - HTTPS limiting significantly the potential surface attacks. The most notable software products that might be targeted for known vulnerability assessments are CloudFront Load Balancer, GlobalProtect, and Palo Alto Networks PAN-O. Dublin VPN website IP 185.240.186.151 (as confirmed also by DNSDumpster) has a login page requiring the client's certificate. The certificate used by the website was issued by palo-sub-ca.corp.reliaquest.com of SH-256 with RSA key size 2048 bit. However, all 3 other Irish addresses do not have the information requiring a valid client certificate although the connection is still not secured requiring installation of certificate.



Host Filters

Labels:

17	ipv6
15	network.device.vpn
8	jquery
8	login-page

Autonomous System:

24	AMAZON-02
13	AMAZON-AES
4	RELIAQUEST
3	ASN-FLEXENTIAL
3	SWITCH-LTD
1	HTIL-TTML-IN-AP Tata Teleservices Maharashtra Ltd
1	LEVEL3
1	RAPIDSYSTEMS

Location:

24	United States
11	United Kingdom
6	India
4	Ireland
3	Brazil
1	Canada
1	Germany

Service Filters

Service Names:

82	HTTP

Ports:

49	443
33	80

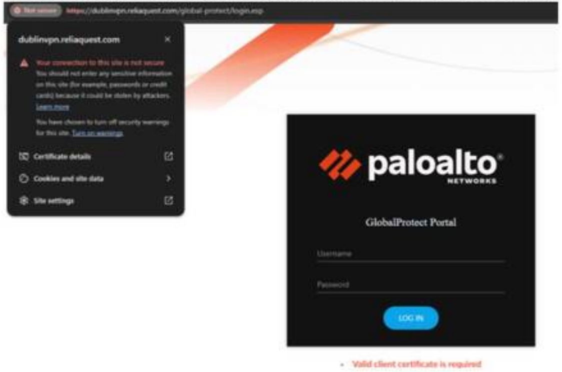
Software Vendor:

36	Amazon
30	Palo Alto Networks
5	nginx
4	Microsoft
2	PHP
1	Apache

Software Product:

34	CloudFront Load Balancer
15	GlobalProtect
15	PAN-OS
5	nginx
2	Elastic Load Balancing
2	HTTP API
2	PHP
2	Windows
1	HTTPD
1	OpenSSL
1	apache

Figure 31: Result report from Censys



https://dublinvpn.reliaquest.com/global-protect/login.esp

dublinvpn.reliaquest.com

Your connection to this site is not secure

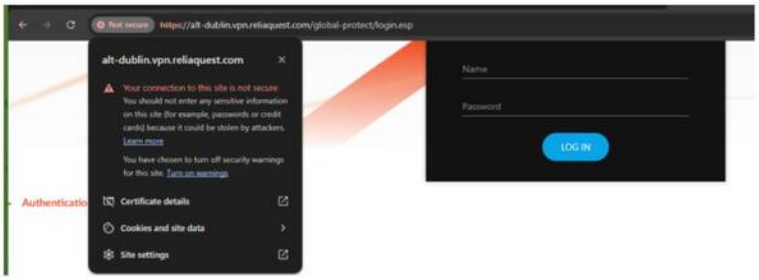
You should not enter any sensitive information on this site (for example, passwords or credit cards) because it could be stolen by attackers.

You have chosen to turn off security warnings for this site.

GlobalProtect Portal

- Valid client certificate is required

Figure 32:Login page to Palo Alto that requires valid client certificate https://185.240.186.151/global-protect/login.esp



https://alt-dublin.vpn.reliaquest.com/global-protect/login.esp

alt-dublin.vpn.reliaquest.com

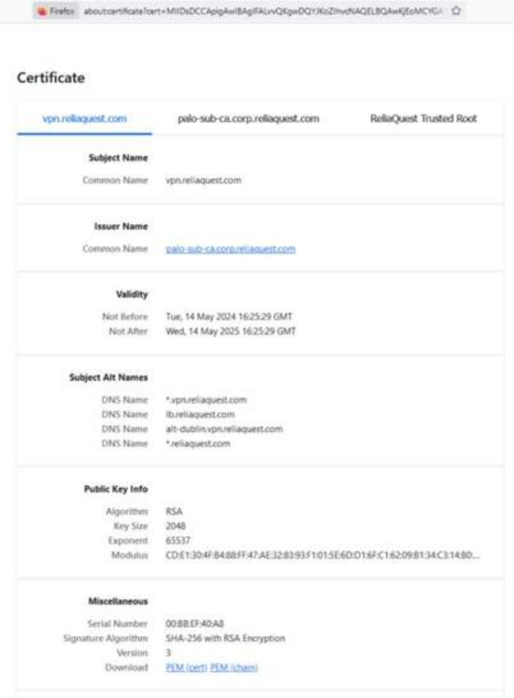
Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards) because it could be stolen by attackers.

You have chosen to turn off security warnings for this site.

- Authenticatio

Figure 33: Login page to Palo Alto that does not have the information requiring valid client certificate



about:certificate?cert=MIIDsDCCApigAwIBAgIFALvvQKgwDQYJKoZIhvcNAQELBQAwKjEoMCYGA

Certificate

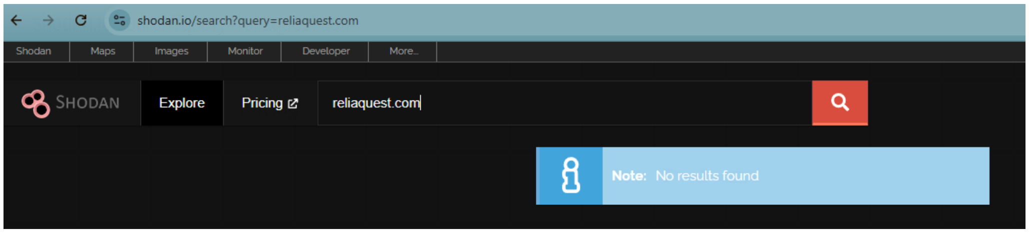
vpn.reliaquest.com | palo-sub-ca.corp.reliaquest.com | ReliaQuest Trusted Root

Subject Name	
Common Name	vpn.reliaquest.com
Issuer Name	
Common Name	palo-sub-ca.corp.reliaquest.com
Validity	
Not Before	Tue, 14 May 2024 16:25:29 GMT
Not After	Wed, 14 May 2025 16:25:29 GMT
Subject Alt Names	
DNS Name	*.vpn.reliaquest.com
DNS Name	lb.reliaquest.com
DNS Name	alt-dublin.vpn.reliaquest.com
DNS Name	*.reliaquest.com
Public Key Info	
Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	CD:E1:30:4F:B4:88:FF:47:AE:32:83:93:F1:01:5E:6D:D1:6F:C1:62:09:B1:34:C3:14:80:...
Miscellaneous	
Serial Number	00:BB:EF:40:A8
Signature Algorithm	SHA-256 with RSA Encryption
Version	3
Download	PEM (cert) PEM (chain)

Figure 34: Details of certificate in https://185.240.186.151/global-protect/login.esp

5.9.Shodan

Shodan is a search engine that regularly scans the Internet for exposed devices, servers, and systems, subsequently indexing the information it finds. It provides the possibility to find services, open ports, and software versions online. There were no results for ReliaQuest or reliaquest.com:



Note: No results found

Figure 35: No results of reliaquest.com

6. Attack Vectors - Mitre ATT&CK framework

6.1.Phishing and Gather Victim Identity Information

The motive behind phishing attacks is to deceive people into providing sensitive information such as a username and password by impersonating a person or entity whom the victim trusts. This can be achieved when personal information or organizational information is compromised and can be utilised to craft highly plausible phishing emails. Examples include threatening emails or urgent money transfer requests by or purportedly by a company's Human Resources department, CEO, IT department, or any other known source such as family members.

The private email address [redacted] of [redacted] was listed in 37 data breaches, including but not limited to ParkMobile 2021 and The Post Millennial 2024. Due to the fact that this email address was involved in breaches across multiple services, it might be a far greater target vector of a phishing attack. It also provides information on services he has and might still be using. This information can also be combined with his public profiles in places such as [redacted] and GitHub to perform spear-phishing.

The report also discovered a number of both internal company personnel (e.g., dwire@reliaquest.com, khill@reliaquest.com) and external partners (e.g., r.benat@eclecticiq.com, reliaquest@highwirepr.com).

MITRE ATT&CK Reference:

- Initial Access:
  - **Phishing [T1566]** A well-known attack tactic for initial access, attackers use phishing to send fake messages that convincingly persuade victims to provide their credentials or click malicious links.
  - **Spearphishing Attachment [T1566.001]** - The target is sent emails with attachments that will execute malware to compromise the system upon opening.
  - **Spearphishing Link [T1566.002] -** Threat actors sent emails with embedded malicious links that will redirect victims to fake login pages or download malware for credential theft or compromise of the system.
  - **Spearphishing Voice [T1566.004]** - This is similar to spearphishing in that the attacker will pretend to be a trusted entity to elicit sensitive information from their target, or otherwise trick them into taking some action against security.

- Reconnaissance:
  - **Gather Victim Identity Information [T1589] -** Relevant to spotting critical identity-related information that relates to ReliaQuest's infrastructure or employees, the attacker can use subdomains, services, or possible OSINT data - such as patterns in email structure or recurring employee names - to further its knowledge about organizational roles and key contacts. This would eventually enable a hacker to craft targeted phishing attacks, impersonate internal services, or spot key people for social engineering.
  - **Email Addresses [T1589.002] -** An attacker might attempt to enumerate or guess e-mail addresses, possibly leveraging subdomain information, typical naming conventions, or OSINT sources in targeting specific individuals within the organization.
  - **Employee Names [T1589.003] -** An attacker may leverage the sub-domain names as a cross-reference from OSINT sources like LinkedIn down to specific individuals, even to the department level. It also aids spear-phishing campaigns; thus, attackers can tailor the message with actual employee names, titles, and departments.

Potential impact: A successful phishing attack may result in credential theft, unauthorized access to sensitive company resources, data exfiltration, or malware infections such as ransomware or keyloggers. Stolen credentials might result in privilege escalation to deliver much more serious attacks - involving data breaches, espionage, or even lateral movement in the network.

Proposed remediation: multi-factor authentication (MFA), phishing awareness training, email filtering and monitoring, and email validation protocols (DKIM, DMARC).

6.2.Credential Stuffing and Password Attacks

Credential stuffing attacks involve the usage of large sets of compromised usernames and passwords, commonly aggregated from previous data breaches, for unauthorized access to accounts on other sites. Most of these attacks depend on password reuse across multiple platforms by users. Attackers also apply password spraying, a type of brute-force attack where only a few common passwords are tried across many different accounts. These attacks are automated and may be performed against systems that do not employ rate limiting or account lockout mechanisms.

The report discovered publicly accessible login pages for various ReliaQuest services (GreyMatter, Digital Shadows), VPN endpoints and login pages including requiring a client certificate and finally [redacted] private email, [redacted] that would be a great candidate for credential stuffing and password attacks as his email appeared in 37 data breaches, most recently in September 2024.

MITRE ATT&CK Reference:

- Brute Force:
  - **Password Guessing [T1110.001]-** This is generally done by an attacker, who would continually try common or weak passwords on an account until the correct password is found, leveraging predictable passwords and/or poor password policies.
  - **Password Cracking [T1110.002]** - If hashed passwords are acquired, such as in the event of a data breach, then it may be possible for attackers to decrypt or "crack" these hashes using offline cracking tools and recover the original passwords of users.

  - **Credential Stuffing [T1110.004]** - Attackers use lists of stolen usernames and passwords, often from other breaches, to try logging in on other sites to take advantage of password reuse across services.

Potential Impact: unauthorized access, compromise of high-privilege accounts, reputation damage, lateral movement within the network.

Proposed remediation: rate limiting and account lockout, password complexity, credential and suspicious login attempts monitoring and user education.

6.3.Exploitation of Web Applications

A web application exploitation generally includes finding a bug in the web application layer of the target and leveraging a vulnerability to an entry point to get unauthorised access, escalate privileges, or exfiltrate sensitive data. An attacker can use these entry points to track user behaviour, intercept data, or even inject malicious scripts.

Most relevant data:

- **Main Website:** www.reliaquest.com uses WordPress as the Content Management System (CMS).
- **JavaScript Libraries:** Utilizes jQuery 3.6.0, GSAP, and core-js 3.36.1.
- **UI Frameworks:** ReliaQuest employs Bootstrap 5.2 and Swiper for its user interface.
- **Tracking and Analytics:** FingerprintJS is in use for user tracking.
- **Hosting and Protocols:** The infrastructure includes HTTP/3 protocol, AWS, Cloudflare Spectrum, and WPEngine for hosting, with various subdomains such as go.reliaquest.com and sl.reliaquest.com.

MITRE ATT&CK Reference:

- Initial Access:
  - **Exploit Public-Facing Application [T1190]** - Attackers utilise publicly accessible application vulnerabilities - Web App in this scenario - to gain unauthorized access. ReliaQuest has several public-facing web applications.
- Persistence:
  - **Web Shell [T1505.003]** - After initial access, attackers may install a web shell. It is also relevant also due to the use of WordPress as the CMS.
- Command and Control:
  - **Application Layer Protocol: Web Protocols [T1071.001]** - Attackers may utilise the default web protocols, such as HTTP/HTTPS, to communicate with a compromised system and attempt to resemble normal traffic. Data exfiltration may also occur in the same manner.

Potential impact: exfiltration of sensitive information within a user session, XSS attacks on vulnerable JavaScript libraries or UI used for session hijacking and code injection and misuse of web protocols could lead to denial of service (DoS).

Proposed remediation: update and patch CMS, libraries and frameworks regularly, enhance input validation, implement web application firewalls (WAFs), conduct routine penetration testing, and use content security policy (CSP) headers.

6.4. Exposed DNS Information & Infrastructure Mapping

This attack vector involves gaining detailed information about DNS records, IP addresses, and associated services. An attacker could exploit this to find potential entry points or vulnerabilities in the network infrastructure for further attacks, which could include targeted phishing, DoS, or exposed service exploitation.

The report identified hundreds of IPs, hosts and a number of subdomains such as go.reliaquest.com, email.reliaquest.com, sl.reliaquest.com, hosting providers (Cloudflare Spectrum, WPEngine), Proofpoint for email filtering and DNS records. This information could be used to map the network by enumerating all accessible services, finding potential entry points for exploits, and conducting reconnaissance to understand the topology of a network, spotting susceptible services hosted.

MITRE ATT&CK Reference:

- Reconnaissance: **Active Scanning [T1595]:**
    - **Vulnerability Scanning [T1595.002]** - This involves active probing of systems and services to look for known vulnerabilities that could be exploited by an attacker-such as versioned or poorly configured systems. In the report, the identified components can be scanned for types of vulnerabilities, such as WordPress and other services identified.
    - **Wordlist Scanning [T1595.003]** - An attacker uses a pre-defined list of common subdomains or directories to attempt to identify accessible web services. The attackers can discover more entry points by scanning for default subdomains and paths.
- **Gather Victim Network Information [T1590]:**
    - **IP Addresses [T1590.005]** - Attackers can enumerate IP addresses associated with a target to determine what the infrastructure boundary is and then, in turn, focus on specific IPs for further exploitation, DoS attacks, or network footprinting.
    - **Domain Properties [T1590.006]** - DNS records, hosting information, and domains could give insight into the infrastructure of a network, enabling attackers to understand network topology and to identify potentially vulnerable third-party hosting services, such as WPEngine or Cloudflare Spectrum.
    - **DNS [T1590.002]** - An attacker may enumerate subdomains, MX records, and other entries through DNS data to help understand the network structure and find additional targets.
- **Acquire Infrastructure [T1583]** - Attackers may attempt to acquire similar infrastructure to impersonate the relevant parts of the environment of ReliaQuest. This might involve the setup of fake domains or IP addresses that are similar to the real ones and could pass controls, thereby deceiving users or employees to communicate with sham sites or services.

Potential Impact: detailed map of the target's infrastructure, identification of less secure entry points or misconfigurations, denial of service, data exfiltration or system compromise

Proposed remediation: Implement DNS security measures (DNSSEC, DNS filtering), split-horizon DNS to separate internal and external DNS information, SPF, DKIM, and DMARC protocols to authenticate emails from the organization’s domain.

6.5.Exploitation of Cloud Services

The dependence on cloud infrastructure opens potential risks for exploitation when configuration, access controls, or authentication protocols in the cloud have not been set correctly. The report confirms that hosting services are outsourced by AWS, Cloudflare Spectrum and WPEngine in addition to SaaS offerings such as GreyMatter and Digital Shadows portals which indicates that portions of the infrastructure depend on cloud service providers. Misconfigurations, open APIs, or poor access controls within these cloud services provide avenues through which attackers can extract sensitive data, disrupt services, or attain further access to more internal resources.

MITRE ATT&CK Reference:

- Initial Access: **Valid Accounts [TA1078.004]** - Adversaries might use the stolen credential to gain unauthorized access to accounts hosted in the cloud. Applicable due to ReliaQuest's use of various cloud services (AWS, Cloudflare, WPEngine) and SaaS offerings (GreyMatter, Digital Shadows portal).
- Execution: **Container Administration Command [T1609]** – Attackers may execute malicious code or commands directly in the cloud environment if access is achieved.
- Persistence: **Create Account: Cloud Account [T1136.003]** - Attackers may maintain access to cloud resources by creating new cloud accounts or modifying the permissions in existing accounts across ReliaQuest's cloud infrastructure.
- Privilege Escalation: **Valid Accounts: Cloud Accounts [T1078.004]** - Once access is gained, adversaries may attempt to employee privilege escalation to obtain access to sensitive information or critical functions in the cloud environment using vulnerabilities or misconfigurations in ReliaQuest's cloud setup.
- Impair Defenses: **Disable or Modify Tools [T1562.001]** - Adversaries may disable cloud-specific security features or logging within cloud provider accounts to avoid detection.
- Data Exfiltration: **Transfer Data to Cloud Account [T1537] -** The threat actors could be interested in cloud storage as a target to exfiltrate sensitive data hosted on services based in the cloud.

Potential Impact: unauthorized access to critical data, service disruption, or data breaches and lateral movement that might result in compromising data integrity, impact operational continuity, and lead to significant financial and reputational damage.

Proposed remediation: Impalement a strong Identity and access management (IAM) policy. MFA to be enabled at all cloud services. Regular auditing and reviewing of configuration settings and access logs to be done. The utilisation of CSPM tools, the principle of least privilege, and data encryption in transit and at rest. Periodic vulnerability assessment and pentesting on cloud infrastructure. Set up adequate logging and monitoring solutions. As disclosed in the report, some of the login pages require additional client's certificate.

7. Conclusions

The OSINT investigation suggests that although ReliaQuest has implemented robust defences, there are critical areas where attention is required. Our findings highlighted a number of potential vulnerabilities and areas of concern which included:

- Employee's information and email addresses are exposed online. This report proved that the Chief Scientist's private email address was part of multiple data breaches leading to potential disclosure of his place of residence, names, passwords, genders, date of birth, licence plates, private messages, phone numbers, IP addresses, geographic locations, partial credit card data, device information, encrypted keys, website activity, creating a higher risk of targeted phishing and breaches.
- A number of different login portals and services are exposed online that could be susceptible to credential stuffing and password attacks. As disclosed in the report, some of the login pages require an additional client's certificate which is good security practice.
- Various cloud services and SaaS offerings are publicly available, presenting potential risks if misconfigured. In addition, a high number of IP addresses and subdomains, plus the use of third-party services, increase the attack surface area.
- DNS and public-facing infrastructure information is publicly available, enabling effective mapping of the core of the company's network).

The potential critical vulnerabilities that were identified included phishing and identity information gathering, credential stuffing and password attacks, exploitation of web applications, exposed DNS information, and cloud service exploitation. Each of the vectors was analysed using the MITRE ATT&CK framework, and relevant techniques included but were not limited to T1110: Brute Force, T1190: Exploit Public-Facing Application, and T1078.004: Cloud Accounts.

This report emphasises that passive reconnaissance facilitates low-risk insight into an adversary's attack surface in a nonintrusive manner that helps an organization take early action. Passive reconnaissance is crucial in detecting those hidden weaknesses and information that could be harder to find with active scanning or through penetration testing. It forms the core of an organization's vulnerability management and incident response to allow swift mitigation. As a prelude to active testing, this report's findings can serve as a foundation for more targeted penetration testing, helping prioritize areas that might otherwise be overlooked.

The digital landscape is ever-changing, and so are the tactics of cyber threats. ReliaQuest is a security company that has to be constantly on guard for the protection not only of its clients but also of itself. This OSINT investigation serves to remind the reader that even organizations focused on security may have vulnerabilities in their public-facing assets. Building a strategy on regular self-assessment, therefore, would provide a mitigation for such problems which will strengthen the security posture of ReliaQuest and its assets, employees, and customers from any potential cyber threats.

8. Appendix 1 – theHarvester output

Output from theHarvester on “ReliaQuest.com” search:

```
{
  "asns": [
    "AS13335",
    "AS13414",
    "AS14618",
    "AS15169",
    "AS15395",
    "AS16509",
    "AS18742",
    "AS209242",
    "AS32934",
    "AS8068"
  ],
  "hosts": [
    "*.reliaquest.com",
    "3de.reliaquest.com",
    "acds.reliaquest.com",
    "agent.reliaquest.com",
    "agentvpn.reliaquest.com",
    "ahm-ca.reliaquest.com",
    "ahm-eu.reliaquest.com",
    "ahm.reliaquest.com",
    "ahm.reliaquest.com:d28kp1t1x0t1fc.cloudfront.net",
    "ahm.reliaquest.com:d28kp1t1x0t1fc.cloudfront.net.",
    "alt-dublin.vpn.reliaquest.com",
    "alt-dublin.vpn.reliaquest.com:185.240.186.154",
    "alt-dublinvpn.reliaquest.com:185.240.186.153",
    "alt-tampadtcvpn.reliaquest.com",
    "alt-tampadtcvpn.reliaquest.com:128.136.211.25",
    "alt-vegasdtcvpn.reliaquest.com",
    "alt-vegasdtcvpn.reliaquest.com:216.115.71.224",
    "alt-vpn.reliaquest.com:128.136.211.24",
    "atf.reliaquest.com",
    "autodiscover.reliaquest.com",
    "autodiscover.reliaquest.com:40.99.58.152",
    "autodiscover.reliaquest.com:40.99.58.24",
    "autodiscover.reliaquest.com:52.98.66.216",
    "autodiscover.reliaquest.com:52.98.89.72",
    "autodiscover.reliaquest.com:autod.ha-autod.office.com",
    "autodiscover.reliaquest.com:autod.ms-acdc-autod.office.com",
    "autodiscover.reliaquest.com:autodiscover.outlook.com",
    "autodiscover.reliaquest.com:autodiscover.outlook.com.",
    "cac1.vpn.reliaquest.com",
    "cac1.vpn.reliaquest.com:99.79.175.200",
    "configs.reliaquest.com",
    "ctf.reliaquest.com",
    "ctf.reliaquest.com:ctfloadbalancer-282171794.us-east-1.elb.amazonaws.com",
    "ctf.reliaquest.com:ctfloadbalancer-282171794.us-east-1.elb.amazonaws.com.",
    "dashlane-sso.reliaquest.com",
    "dublinvpn.reliaquest.com",
    "dublinvpn.reliaquest.com:185.240.186.151",
    "edl.reliaquest.com",
    "email.reliaquest.com",
    "euc1.vpn.reliaquest.com",
    "euc1.vpn.reliaquest.com:3.74.119.42",
    "eun1.vpn.reliaquest.com",
    "eun1.vpn.reliaquest.com:13.50.55.144",
    "euw2.vpn.reliaquest.com:3.11.188.74",
    "events.reliaquest.com",
    "gmdemo.reliaquest.com",
    "go.reliaquest.com",
    "info.reliaquest.com",
    "info.reliaquest.com:ab46.mktossl.com",
    "info.reliaquest.com:reliaquestllc.mktoweb.com",
    "info.reliaquest.com:reliaquestllc.mktoweb.com.",
    "intel.reliaquest.com",
    "itsecurity.reliaquest.com",
    "lb.reliaquest.com",
    "lb.reliaquest.com:44.207.56.190",
    "lyncdiscover.reliaquest.com",
    "mail.reliaquest.com",
    "mail.reliaquest.com:208.38.160.195",
    "parse.reliaquest.com",
    "partners.reliaquest.com",
    "portal.reliaquest.com",
    "resources.reliaquest.com",
    "rq-ssl-dtct.reliaquest.com",
    "rq-ssl-dtct.reliaquest.com:128.136.211.22",
    "rq-ssl-socv.reliaquest.com",
    "rq-ssl-socv.reliaquest.com:24.120.116.182",
    "rqa.reliaquest.com",
    "rqa.reliaquest.com:18.232.221.204",
    "security.reliaquest.com",
    "sip.reliaquest.com",
    "sl.reliaquest.com",
    "sl.reliaquest.com:custom-tracking.salesloft.com",
    "sl.reliaquest.com:custom-tracking.salesloft.com.",
    "sync.reliaquest.com",
    "sync.reliaquest.com:d33mplw87lqqky.cloudfront.net",
    "sync.reliaquest.com:d33mplw87lqqky.cloudfront.net.",
    "tampadtcvpn.reliaquest.com",
    "tampadtcvpn.reliaquest.com:128.136.211.23",
    "tampahqvpn.reliaquest.com:198.92.96.250",
      "tlg.reliaquest.com",
      "u.reliaquest.com",
      "use1.vpn.reliaquest.com:44.207.56.190",
      "vegasdtcvpn.reliaquest.com",
      "vegasdtcvpn.reliaquest.com:64.79.128.69",
      "vegasvpn.reliaquest.com",
      "vegasvpn.reliaquest.com:24.120.116.183",
      "vpn.reliaquest.com:64.79.128.69",
      "vpn.reliaquest.com:lb.reliaquest.com",
      "vpn.reliaquest.com:lb.reliaquest.com.",
      "web.reliaquest.com",
      "web.reliaquest.com:247765.webhost13.hubspot.net",
      "web.reliaquest.com:247765.webhost13.hubspot.net.",
      "webmail.reliaquest.com",
      "whitepaper.reliaquest.com"
   ],
   "emails": [
      "dwire@reliaquest.com"
   ],
   "interesting_urls": [
      "https:\/\/email.reliaquest.com\/images\/downloadPicture.gif",
      "https:\/\/email.reliaquest.com\/track?mktoTestLink&mkt_tok=NDM4LUtZSy03ODYAAAGS2XAQlY--ojtNMJaMaZ0R97D9AGpxgRgVmu-_zrokqoExwSn5pctOGE5UW0ti1cIs8HNLGt2DoZbOFt1EjR3vVzbhZBCdykvg5xh7Z6J8LeJp",
      "https:\/\/email.reliaquest.com\/track?mktoTestLink&mkt_tok=NDM4LUtZSy03ODYAAAGSgMLqrijI4X7FMUcUXuSGq90ObnYRwXEYLjLSoL6EvW5fbOHJPJbrMbQEuwTlYa8P8SlJ-nxsCx0ItvsAk8UeWBpIV0t8gHhM4GrBfIQnpBfV",
      "https:\/\/email.reliaquest.com\/track?mktoTestLink&mkt_tok=NDM4LUtZSy03ODYAAAGUYgEWAkilskR42lRGruuCw6GecrkNcmprkXJyeP58GVRhaQV0dcphAGf-5wtWCJ-NOuwKCyfVUhpw6C3C8-E2LsmPcPPX8ES-4WQYBlGT8Br8",
      "https:\/\/email.reliaquest.com\/track?mktoTestLink&mkt_tok=NDM4LUtZSy03ODYAAAGUo5MT2N-XZ5EWPcuumV3JywwxdSMgTGGonKrBm09SyH0c1kSDuxS3Y5BVLp6AmfSIAKHGl0MqIdY6_rHNbaOBS6EzLoCHTv1mQ5tbb4kfSJve",
      "https:\/\/email.reliaquest.com\/track?mktoTestLink&mkt_tok=NDM4LUtZSy03ODYAAAGVYnLyVYowPC4hbiObW3w0Z_qFH6Oh3UJ0QvU-0B3DpvHs_pEQ3DYiRu-D5xeUGHUFWVzy5lGhfRFkEQJSxF9copxexEPMsHxqHTMoboNq_kna",
      "https:\/\/email.reliaquest.com\/track?mktoTestLink&mkt_tok=NDM4LUtZSy03ODYAAAGVzbkKTWOywoYaiR3s2tnNNixRKDcV6toXX_0QNf1JhmgO9Bi4AzpKBg271GjWURrL-AuRB9Q27VZFuBwmAJyc0jALeBXkZV4UlqmrrHoi_T8k",
      "https:\/\/email.reliaquest.com\/trk?t=1&amp;mid=NDM4LUtZSy03ODYAAAGS2XAQleBPZeV-UGD2bzt5flgk9a0upMwff-UYk4vl7Pr0whKFX56GT5kCFHD_AlYCKv05Wg2eTlNKdZ7KSqeHbdBUdyTOYU6tQzj2nbiJNy_gcYI9mx7HMr05fpsVYDM4kBYpVQDUjl_Gm5bHPI1FIA",
      "https:\/\/email.reliaquest.com\/u\/NDM4LUtZSy03ODYAAAGS2XAQlYyk1-IGeUu_Aq5jaYwmjDryty-x4kT6fopCWJu5VDqGTukBWCzMYFdcQ9LAbrFnm9w=?emailAddress=NDM4LUtZSy03ODYAAAGS2XAQlVFbA2cmj0dzXRbLE6rbd-_4rUDHOLpI6kBN9w8UWDyfycosxeiYoO_NmhLw8_2rcxzhIbNO",
      "https:\/\/go.reliaquest.com\/Preference-Management_2024.html?mkt_tok=NDM4LUtZSy03ODYAAAGUo5MT2HzKLDPhGh_YmhHlOBdRujAdIx3xEFKWpG-8TPlkAA4Tyh0lB3mAwt5FyJwTFhwbx53sZn100MB8mdB_8k6dKRapY3ioOAJ0nhSOwpsp",
      "https:\/\/go.reliaquest.com\/preference-center-new.html?mkt_tok=NDM4LUtZSy03ODYAAAGUo5MT2Jifp-clzWHcAUbcKijVbc_4XmZkdqjNVaAtqT-jZuP4sXjEyNFzjhRK30-KHs-t9R09pUK5OZ1XyWx3FPeEsNXg3InaaENiafuzjTN1",
	"https:\/\/go.reliaquest.com\/preference-center-new.html?mkt_tok=NDM4LUtZSy03ODYAAAGVYnLyVQQE3_EbRUrXUi9BT30U6zQZNETainZdUp61amAVzIMKSGeL48D0YaMvgQC4I07PvxYLp-nx3FG2tB2DJYkTxwYc0Yw_SVI6zCkB3VXd",
	"https:\/\/go.reliaquest.com\/preference-center-new.html?mkt_tok=NDM4LUtZSy03ODYAAAGVzbkKTQA1oUhrMFqvqEw5W5TEFHmttoBk44d2Fsap8Ynxip4g-S-VbZEYlXNcVZ0Qs7d0KGd88i6UfQVqS41SKC5iS2pu74Y-ACNjOmFo3xOc",
	"https:\/\/go.reliaquest.com\/preference-center.html?mkt_tok=NDM4LUtZSy03ODYAAAGS2XAQlZfleL_PHuo_jZg9jBZ_1vB30VzIFGG43CMXbNW67Vpw3MAWDaDIMFjpuvbgzZODGYhDkyPbgcpS8pjX2qAqzQsn8menwaWvaT-_MNnl",
	"https:\/\/go.reliaquest.com\/preference-center.html?mkt_unsubscribe=1&amp;mkt_tok=NDM4LUtZSy03ODYAAAGS2XAQlU9IAhQnwi-YKNHgF6CSLj601uh2u8hL6RxoRDvHLPi8wZt7uwvkfpICpOX-FXnUhPp72VAPj_a_uYCrrZeEd4JZes3VhDerpVqy6KNS",
	"https:\/\/go.reliaquest.com\/preference-center.html?mkt_unsubscribe=1&mkt_tok=NDM4LUtZSy03ODYAAAGS2XAQlU9IAhQnwi-YKNHgF6CSLj601uh2u8hL6RxoRDvHLPi8wZt7uwvkfpICpOX-FXnUhPp72VAPj_a_uYCrrZeEd4JZes3VhDerpVqy6KNS",
	"https:\/\/go.reliaquest.com\/preference-center.html?mkt_unsubscribe=1&mkt_tok=NDM4LUtZSy03ODYAAAGT71WiN0wx7uk6qYuV6nBylJUdlgu5f0bJQKzScOwd2kslqYGzaXS3vBDWLGbVwCiPMetcUcOcvpVOd4WXTMVlha6um8f0juONIFBTFTGa8x5r",
	"https:\/\/go.reliaquest.com\/preference-center\/",
	"https:\/\/go.reliaquest.com\/rs\/438-KYK-786\/images\/Email%20Header%20-%20SOC%20Talk_%20Automating%20Threat%20Response%20-%20600x236%20-%20US.png?version=0",
	"https:\/\/go.reliaquest.com\/rs\/438-KYK-786\/images\/FY25Q2_JulyCNL_Blog2.png?version=0",
	"https:\/\/go.reliaquest.com\/rs\/438-KYK-786\/images\/RQTR_100324_IntelligenceSummary.pdf?version=0?utm_source=marketo&utm_medium=email&utm_campaign=fy25q3_intelligence_summary_report&utm_content=intelligence-summary&mkt_tok=NDM4LUtZSy03ODYAAAGV8TyiDVvRmwgUi2JE1-3kbjELd1XfT3hHhitoAdRLIr6iwx7X2tG-tGVt_D5-_1ACtKRJAgETU-o3wp5uNpm3ozCf8J9mogG2EauR-mrs8ZF2",
	"https:\/\/sl.reliaquest.com\/",
	"https:\/\/www.reliaquest.com\/",
	"https:\/\/www.reliaquest.com\/?mkt_tok=NDM4LUtZSy03ODYAAAGUo5MT2ITdmv9Gk7v9gxZdQUDKouHOIDrfFR2WDSApBAeeMWPgPzcg6vjGGdT8b6ppGNP0FvF-Hmq4fq6h-RanVbe-z7tfju_y-B20oKRGEm2v",
	"https:\/\/www.reliaquest.com\/?utm_source=marketo&utm_medium=email&utm_campaign=event-email&utm_content=home-page&mkt_tok=NDM4LUtZSy03ODYAAAGUo5MT2QaRG64ArRRWET-OToMI3Ce4u_xOdMX01PvdkyzFpt3APSoQPZdyNgFcNIX0BjrrDh4LpA86s7DePTTzCSLrSCaSwRMkUMJNQStkn-bo",
	"https:\/\/www.reliaquest.com\/?utm_source=marketo&utm_medium=email&utm_campaign=nurture-email&utm_content=home-page&mkt_tok=NDM4LUtZSy03ODYAAAGS2XAQlZrou0tSn9urRbAiQEOSzH9QFaVgT1fC1CNLKeKm74TwBOznE9ntIRnas2_ZhxwZsDcAKr_nHYDkNadN_91QF8MiXQ1ByATQFJf45iVk",
	"https:\/\/www.reliaquest.com\/?utm_source=marketo&utm_medium=email&utm_campaign=nurture-email&utm_content=home-page&mkt_tok=NDM4LUtZSy03ODYAAAGVYnLyVUu5bPIIW87kiP0nXrEd_2B2Ms7Rb_PjtblYJZp7A-Zb8M7kCqJnvvLDR2bnJtXDsuioN0wpfnFaL428IwU8uq-B3BCEeyvwj93DkQbm",
	"https:\/\/www.reliaquest.com\/?utm_source=marketo&utm_medium=email&utm_campaign=nurture-email&utm_content=home-page&mkt_tok=NDM4LUtZSy03ODYAAAGVzbkKTZx94y97hVUpCd_qACCPxikIRmywNVjIDzh5IFszbgNfUKOZ0xNBHek_5FfjwcBb_pcYXau7JdNySKVeGhIyftbn1bN97PkZ1jxe8_7k",
	"https:\/\/www.reliaquest.com\/blog\/black-basta-social-engineering-technique-microsoft-teams\/",
	"https:\/\/www.reliaquest.com\/blog\/blacksuit-attack-analysis\/",
      "https:\/\/www.reliaquest.com\/blog\/crowdstrike-outage-script-phishing-and-social-engineering-attacks\/",
      "https:\/\/www.reliaquest.com\/blog\/crowdstrike-outage-script-phishing-and-social-engineering-attacks\/?utm_source=marketo&utm_medium=email&utm_campaign=fy25q2_july_prospect_nl&utm_content=blog&mkt_tok=NDM4LUtZSy03ODYAAAGUo5MT2JKq-pvcLfwsBlnqIpQ_OTI7JWZc6hDEDBINAIkmo03uXf07U_hmCDZV903m7CP65fVqBvu-AQM9HxKH4beNca1863evpZUaIBERHa4A",
      "https:\/\/www.reliaquest.com\/blog\/medusa-attack-analysis\/?utm_source=marketo&utm_medium=email&utm_campaign=fy25q2_july_prospect_nl&utm_content=blog&mkt_tok=NDM4LUtZSy03ODYAAAGUo5MT2Ol8go74QW_vqouvHVQJSRfr5gXzj8Sr5_YnnaItES55sSI0WvQ3DonPg1tqLdxM4xcJTfcRdbCpxt8He1ZBrRqhMG9nfECr2tkJGMol",
      "https:\/\/www.reliaquest.com\/blog\/new-execution-technique-in-clearfake-campaign\/",
      "https:\/\/www.reliaquest.com\/blog\/q1-2024-ransomware\/",
      "https:\/\/www.reliaquest.com\/blog\/q2-2024-ransomware\/",
      "https:\/\/www.reliaquest.com\/blog\/q2-2024-ransomware\/?utm_source=marketo&utm_medium=email&utm_campaign=fy25q2_july_prospect_nl&utm_content=blog&mkt_tok=NDM4LUtZSy03ODYAAAGUo5MT2Y6loWq0O4wr4Dyk1xwh4rVyF6TGKXjfuaILKFtzB1_0GCkBZ0_XYCViMQWHi1UJZvCHcCfz6DFxPLLuQ4W-jnRM5XTBcPpeiXcaM3rC",
      "https:\/\/www.reliaquest.com\/news-and-press\/reliaquest-and-aon-collaborate-to-empower-organizations-to-proactively-manage-cyber-risk\/",
      "https:\/\/www.reliaquest.com\/news-and-press\/reliaquest-launches-first-autonomous-self-learning-ai-agent-for-security-operations\/?utm_source=marketo&utm_medium=email&utm_campaign=fy25q3_eliminatingt1t2_drip&utm_content=press-release&mkt_tok=NDM4LUtZSy03ODYAAAGVzbcel36dqBD-Aczvnl8AoS1lROecBf20oBLOMq6D8iQiqHNiGN6BVsSK2XdxScC-_rquyFLU-SK5As_H5Vsu48dvjQyREv9nyXUTUjZv_Fr2",
      "https:\/\/www.reliaquest.com\/news-and-press\/reliaquest-launches-first-autonomous-self-learning-ai-agent-for-security-operations\/?utm_source=marketo&utm_medium=email&utm_campaign=fy25q3_eliminatingt1t2_drip&utm_content=press-release&mkt_tok=NDM4LUtZSy03ODYAAAGVzbkKTecgDQoNYsgbEE7qXPPXXM2sBXRE61W8Yr0WnCTIbBBPu4SFeodxRqK8bZr6NDNNRwQTlQRhwnsy55h91wpZnC-VoO5p-GahOsXO_Ahv",
      "https:\/\/www.reliaquest.com\/request-a-demo\/",
      "https:\/\/www.reliaquest.com\/resources\/events-webinars\/",
      "https:\/\/www.reliaquest.com\/resources\/research-reports\/ai-powered-cybercrime\/",
      "https:\/\/www.reliaquest.com\/wp-content\/uploads\/2024\/03\/2024-ReliaQuest-Annual-Threat-Report-4.pdf"
   ],
   "ips": [
      "104.17.70.206",
      "104.17.71.206",
      "104.17.72.206",
      "104.17.73.206",
      "104.17.74.206",
      "104.199.122.78",
      "104.244.42.1",
      "104.244.42.129",
      "104.244.42.193",
      "107.23.143.9",
      "107.23.90.191",
      "108.138.94.100",
    "108.138.94.52",
    "108.138.94.62",
    "108.138.94.68",
    "131.253.161.203",
    "132.245.37.136",
    "134.0.78.4",
    "134.170.54.15",
    "134.170.54.18",
    "141.193.213.20",
    "141.193.213.21",
    "165.254.206.67",
    "172.217.18.14",
    "18.188.172.160",
    "18.204.32.217",
    "18.211.113.67",
    "18.65.229.129",
    "18.65.229.25",
    "18.65.229.42",
    "18.65.229.60",
    "184.106.243.51",
    "184.84.180.16",
    "184.84.180.35",
    "198.74.57.142",
    "199.83.44.71",
    "204.2.193.137",
    "204.2.222.122",
    "204.246.191.102",
    "204.246.191.105",
    "204.246.191.106",
    "204.246.191.114",
    "204.246.191.115",
    "204.246.191.120",
    "204.246.191.125",
    "204.246.191.17",
    "204.246.191.25",
    "204.246.191.27",
    "204.246.191.35",
    "204.246.191.41",
    "204.246.191.42",
    "204.246.191.43",
    "204.246.191.50",
    "204.246.191.52",
    "204.246.191.54",
    "204.246.191.7",
    "204.246.191.78",
    "204.246.191.8",
    "204.246.191.80",
    "204.246.191.83",
    "204.246.191.91",
    "204.246.191.92",
    "204.246.191.98",
    "216.206.30.11",
    "23.136.192.215",
    "23.63.227.152",
    "23.63.227.160",
    "23.63.227.210",
    "2600:9000:225e:1c00:18:1695:b600:93a1",
    "2606:4700:4400::6812:2929",
    "2607:f8b0:4004:c0b::88",
    "2620:1ec:21::14",
    "2a00:1450:4001:80b::200e",
    "2a00:1450:4001:810::200e",
    "2a00:1450:4001:813::200e",
    "2a03:2880:f176:181:face:b00c:0:25de",
    "2a03:2880:f176:84:face:b00c:0:25de",
    "2a03:2880:f177:185:face:b00c:0:25de",
    "3.163.158.2",
    "3.163.158.21",
    "3.163.158.6",
    "3.163.158.60",
    "3.209.95.254",
    "3.211.19.236",
    "3.213.223.212",
    "3.214.213.33",
    "3.219.134.181",
    "3.224.190.181",
    "3.224.215.146",
    "3.225.36.146",
    "3.230.38.166",
    "3.232.130.255",
    "3.234.34.245",
    "34.194.158.33",
    "34.194.62.134",
    "34.195.53.28",
    "34.197.13.85",
    "34.203.156.246",
    "34.232.120.137",
    "35.223.154.68",
    "40.96.7.120",
    "40.97.116.88",
    "40.97.119.168",
    "44.216.66.123",
    "52.200.167.119",
    "52.207.45.13",
    "52.21.104.0",
    "52.44.155.238",
    "52.6.96.255",
    "54.146.17.105",
    "54.156.16.178",
    "54.192.73.120",
    "54.192.73.25",
    "54.192.73.27",
    "54.192.73.32",
    "54.192.73.44",
    "54.192.73.47",
    "54.192.73.96",
    "54.192.73.97",
    "54.192.75.15",
    "54.192.75.33",
    "54.192.75.80",
    "54.192.75.92",
    "54.192.76.10",
    "54.192.76.106",
    "54.192.76.121",
    "54.192.76.123",
    "54.192.76.39",
    "54.192.76.46",
    "54.192.76.51",
    "54.192.76.70",
    "54.192.76.78",
    "54.192.76.79",
    "54.192.76.82",
    "54.192.76.97",
    "54.204.135.149",
    "54.205.250.21",
    "54.230.126.10",
    "54.230.126.107",
    "54.230.126.27",
    "54.230.126.64",
    "54.230.126.66",
    "54.230.126.82",
    "54.230.126.89",
    "54.230.126.97",
    "54.243.66.160",
    "54.85.40.143",
    "54.85.40.175",
    "54.85.73.22",
    "63.158.227.33",
    "63.216.54.153",
    "63.216.54.186",
    "65.172.31.56",
    "99.84.66.14",
    "99.84.66.34",
    "99.84.66.35",
    "99.84.66.40",
    "99.84.66.72",
    "99.84.66.73",
    "99.84.66.76",
    "99.84.66.95",
    "99.84.74.108",
    "99.84.74.129",
    "99.84.74.25",
    "99.84.74.36",
    "99.84.74.4",
    "99.84.74.46",
    "99.84.74.47",
    "99.84.74.75"
  ],
  "shodan": []
}
```