Apollo Information Systems, Corp

1 Chisholm Trail Rd, Suite G100
Round Rock, TX 78681
(408) 399-5110 | apollo-is.com

Tarrant Appraisal District

Incident Response Report

January 26, 2024

INTELLECTUAL PROPERTY NOTICE

Apollo Information Systems, Corp

1 Chisholm Trail Rd, Suite G100
Round Rock, TX 78681
(408) 399-5110 | apollo-is.com

Table of Contents

Executive Summary **1**
Introduction 1
Major Incident Takeaways 1
Summary of Events **2**
Anatomy of the Attack 2
Reconnaissance 2
Containment Activities 2
Information Exposure and Exfiltration Analysis 2
Remediation 2
Analysis Details **3**
Objectives 3
Methodology 3
Attack Timeline 3
Vulnerabilities 4
Conclusion **6**
Appendix A – IPs POSTing the "evil.php" Webshell **7**
Appendix B – IPs Executing Directory Transversal Attacks **8**
Appendix C – IPs that Failed to Upload a Webshell **12**

Executive Summary

Introduction

During the Fall of 2022, Tarrant Appraisal District experienced a cybersecurity incident impacting website services. The website was again unavailable during April and May of 2023, with serious accusations of mismanagement made against individuals within the Tarrant Appraisal District technology leadership. Tarrant Appraisal District engaged Apollo Information Systems Corp. (Apollo) on September 6, 2023 to provide incident response and analysis services.

Apollo's objectives were to:

- Determine the initial intrusion vector and time.
- Determine threat actor tactics, techniques, and procedures (TTP).
- Determine if threat actors were active in the network or had established persistent access.
- Determine whether data was accessed or exfiltrated.
- If necessary, provide guidance on containment, eradication, and recovery measures.

Apollo took the following steps to achieve these objectives:

- Coordinated with Tarrant Appraisal District to gain access to all applicable log and security data.
- Analyzed available and relevant evidence to identify threat actor activity.
- Investigated evidence to understand and attempt to develop an incident timeline.
- Examined multiple endpoints for forensic artifacts of the incident.

Major Incident Takeaways

Patient Zero

Patient zero is defined as identifying the initial source of an attack. In this case, Apollo was unable to definitively determine a patient zero.

Data Exfiltration Status

Apollo did not find direct evidence of data theft/exfiltration associated with this incident. However, data was available through vulnerabilities on the website. Analysts assess with medium confidence that data was not stolen.

Threat Actor Persistence

Analysts discovered minimal evidence of threat actor activity on the systems. The website and network were depreciated in April 2023. There are no indications of ongoing persistence.

Summary of Events

Anatomy of the Attack

Apollo was not able to pinpoint the initial intrusion vector because critical evidence was unavailable during the investigation. The evidence was unavailable due to the time lapse from when the incident occurred and when the investigation started. Threat actor activity spanned across multiple endpoints, but www-Happe-90 saw most of the activity. Another endpoint with clear threat actor activity was NFS-101-Server.

Reconnaissance

After a review of Tarrant Appraisal District's triage data and logs, Apollo could not determine if there was reconnaissance of systems before the attack.

Containment Activities

Tarrant Appraisal District attempted immediate containment in October 2022 by taking the website down and creating a sanitized server to put it back online. Then an interim site was used from December 2022 to April 2023, with the original website servers being taken offline.

Information Exposure and Exfiltration Analysis

During the investigation, Apollo performed forensic analysis of multiple endpoints that were part of the old website network. Analysts also examined provided logs for additional connections or evidence of data exfiltration. Direct evidence of exfiltration including searching for data, lateral movement, data compression, or data hoarding was not found.

Remediation

Tarrant Appraisal District's initial response to the incident was ineffective. The source of the malicious activity was not identified, and remediation efforts destroyed evidence. The vulnerabilities that were potential causes of the incident were not discovered nor fixed to prevent additional activity from occurring.

In April 2023, all the systems associated with this investigation were taken offline and a new website was brought online. The standup of a new website removed the vulnerabilities identified later in this report. Apollo analysts did not assess the new website network.

Darknet Data Survey

Apollo's investigation to find TAD-specific confidential data available on the darknet can only be considered "low confidence of attribution." There have been numerous breaches of Texas citizens' personally identifiable information, so it is difficult to determine the leak sources.

A cursory darknet survey of illicit data broker sites returned inconclusive results attributable to TAD. The most common data including addresses of citizens within Tarrant County persists from the SiegedSec leak of Fort Worth's CRIS data on June 26, 2023. An in-depth darknet survey of threat actor and data broker sites would have a low probability of determining leak sources.

Analysis Details

Objectives

The objectives of Apollo's analysis were to determine:

- If and when the threat actor gained access.
- If and how threat actors were able to move laterally within the network.
- If threat actors accessed or exfiltrated any data.

Apollo's goal was to gain an understanding of the tactics, techniques, and procedures (TTP) the threat actor used. The investigation was limited to information available in software and system log files. Due to this limited information, many details of the attack cannot be determined.

Methodology

Apollo followed best practices for responding to cybersecurity incidents including log analysis and host machine digital forensics. The initial analysis began on September 14, 2023, using documents and logs within individual endpoints. Apollo analysts reviewed audits, activity logs, and other forensics artifacts for the targeted endpoints. Indicators from this data directed analysts to areas of interest.

Attack Timeline

This timeline details Apollo's observations about key threat actor activity and TTPs. The timeline is organized according to phases of the threat actor's reconnaissance, preparation, and execution.

Phase 1 – Reconnaissance and Access

There was no evidence of threat actor activity performing reconnaissance activities of probing, scanning, or otherwise observing the Tarrant Appraisal District website network.

Apollo analysts found a remote access tool running in the www-Docker server. The installation configuration of this tool caused analysts to assess with high confidence that this was part of Ardent Creative's, the website contractor, solution for monitoring the health of the website components. The tool is classified as a "hacker tool" used to create backdoors with persistence and was exposed to the internet. No malicious activity was found with this tool, however the use is non-standard and against common security practices.

On April 20, 2022, initial access attempts by the threat actor were on two endpoints: NFS-101-Server, and www-Happe-90. NFS-101-Server logs showed a failed attempt to upload a file named "69.php." Searches for this file and its contents across all PHP files were negative, with no results found.

Endpoint www-Happe-90 showed multiple successful attempts in the logs to connect to an "evil.php" file. No further follow-on activity from the threat actor was found in the evidence provided.

Apollo analysts found logs from June 13 and August 3, 2022, indicating failed attempts to access the "evil.php" files. No additional activity from the threat actors was found in the evidence.

Phase 2 – Malicious Activity

Apollo analysts did not find evidence of malicious activity occurring within the Tarrant Appraisal District website network in the evidence provided.

All activity in the evidence was from outside poor reputation IPs attempting to act on exposed applications. This was across the applications utilized to display the website – WordPress and its plugins, and the MariaDB.

Phase 3 – Breach

Apollo analysts did not find evidence of a data breach in the evidence provided. Due to multiple poor configuration choices, data including usernames and passwords for internal Tarrant Appraisal District resources were available on the internet.

Phase 4 – Response and Recovery

In October 2022, the website was taken down to address the incident. A landing page was displayed while a sanitized server was created. This remediation is not in line with best practices, and we assess with high confidence this led to the loss of evidence that could have been useful in the investigation. Tarrant Appraisal District personnel were unable to positively determine if the images provided to Apollo were taken before this sanitization took place.

Additional Evidence

From October 2022 to January 2023, malicious traffic exiting from IP 12.182.207.108, identified as a TAD SFTP server, was captured by Nomic Networks Intrusion Detection/Prevention Systems that reside just outside the Tarrant Appraisal District website network. These traffic patterns appeared to be automated and not part of employee or normal website activities.

This network traffic exited the Tarrant Appraisal District website network to 22,281 external IPs, causing alerts for attempted exploit activity. The bulk of this traffic was from October 26 through November 3, 2022. Apollo analysts were informed that this endpoint was replaced during the upgrades in April 2023.

Vulnerabilities

Operating Systems

All endpoints from the former website were running a version of Red Hat Enterprise Linux (RHEL), though the version was not standardized across servers. The catalog of versions is:

Hostname	Operating System	Kernel	Vulnerabilities
NFS-101-Server	RHEL 7.4	3.10.0-693.21.1.el7_4.x86_64	10 critical vulnerabilities, 20 additional vulnerabilities
www-Happe-90	RHEL 8.0	4.18.0-80.7.2.el8_0.x86_64	48 critical vulnerabilities, 628 additional vulnerabilities

Hostname	Operating System	Kernel	Vulnerabilities
www-Docker and www-Server endpoints	RHEL 8.0	4.18.0-80.11.2.el8_0.x86_64[1]	48 critical vulnerabilities, 628 additional vulnerabilities
www-ElasticSearch1-92	RHEL 8.1	4.18.0-80.11.2.el8_0.x86_64	4 medium vulnerabilities
www-MariaDB-96	RHEL 8.1	4.18.0-147.0.3.el8_1.x86_64[2]	4 medium vulnerabilities

Docker Versions

Multiple endpoints had Docker[3], a virtualized environment for minimal applications inside "containers," that originated in 2019 and 2021. There was no administrative software that is usually associated with high-availability websites to control updates, or files showing how the containers were built. These findings are not in line with best practices for administrating a website. Analysts assess that the software for running the applications serving the website has likely not been updated since the containers were created.

Software Versions

WordPress was the main application serving the webpage and was version 5.9.3, which has multiple vulnerabilities including Cross-Site Scripting (XSS), SQL injection, and inadvertent data exposure. When the site was replaced in April 2023, the most current version was 5.9.7. As of December 2023, the current stable version is 6.4.2.

Formidable Forms Plugin for WordPress was version 5.2.01, which has multiple vulnerabilities including remote code execution and arbitrary plugin installation. When the site was replaced in April 2023, the most current version available was 6.3.

HAProxy was used on www-HAPPE-90 and the most internet-facing endpoint. The version installed was 1.9r1, which had eight reported vulnerabilities including four that are considered critical. When the site was replaced in April 2023, the most current version available was 2.8LTS.

Memcached containers were created on various days, with the oldest being October 17, 2019, and the newest being October 30, 2020. These align with versions 1.5.19 and 1.6.8. When the site was replaced in April 2023, the most recent version of Memcached was 1.6.20. Six medium vulnerabilities are present in the various versions of this software.

Elastic Search was installed as a container at version 7.9.3, which was released on October 16, 2020. There are seven vulnerabilities present in this version of the software with medium and low ratings. When the site was replaced in April 2023, the most current version was 8.8.0.

[1] This kernel is vulnerable to a privilege escalation vulnerability that a patch was released for in Oct 2020. https://access.redhat.com/security/cve/cve-2020-14386

[2] This kernel is vulnerable to a kernel memory corruption that could lead to privilege escalation. https://access.redhat.com/security/cve/CVE-2019-0155

[3] https://en.wikipedia.org/wiki/Docker_(software)

Maria-DB was installed directly onto the operation systems of www-MariaDB-96 as version 10.3.17 (MySQL 15.1). This version has 73 vulnerabilities, with two critical, including remote code execution. When the site was replaced in April 2023, the most current version was 10.11.3.

Conclusion

In conclusion, the incident response produced the following outcomes associated with the established objectives.

Outcomes

The analysis aimed to determine if threat actors remained active in the network or had established persistent access. After analysis, Apollo determined that the threat actors likely do not have access to the network since the old infrastructure was replaced. Note that this investigation did not include the network that was implemented during April 2023.

The analysis aimed to determine the intrusion vector and time. Apollo found evidence of activity starting in April 2022. However, Apollo was not able to identify the definitive time and vector of malicious activity.

The analysis aimed to determine the tactics, techniques, and procedures (TTPs) the threat actor used to maneuver within the network as well as the associated timeline. There was no evidence of lateral movement within the network from server to server. All evidence suggests that direct connections from outside the network to unprotected and vulnerable servers took place.

The analysis aimed to determine whether data exfiltration occurred. Apollo found no evidence of data exfiltration by threat actors. However, the website as configured before April 2023 would have allowed a threat actor to transverse the multiple servers and possibly extract data. Additionally, a threat actor could have modified logs to hide activity due to no log aggregation tooling, or internal monitoring of the website network.

Appendix A – IPs POSTing the "evil.php" Web Shell

IP address – Country of origin – Hosting provider

104.131.56.45 – US – Digital Ocean	157.245.130.211 – US – Digital Ocean	164.92.92.51 – US – Digital Ocean
104.131.56.48 – US – Digital Ocean	159.223.132.96 – US – Digital Ocean	164.92.98.1 – US – Digital Ocean
104.131.56.73 – US – Digital Ocean	159.223.164.233 – US – Digital Ocean	167.99.57.137 – US – Digital Ocean
104.131.56.93 – US – Digital Ocean	159.223.204.244 – US – Digital Ocean	167.99.59.72 – US – Digital Ocean
104.248.239.181 – US – Digital Ocean	161.35.48.16 – US – Digital Ocean	178.128.149.201 – US – Digital Ocean
137.184.10.255 – US – Digital Ocean	164.92.100.60 – US – Digital Ocean	178.128.157.246 – US – Digital Ocean
137.184.116.128 – US – Digital Ocean	164.92.100.61 – US – Digital Ocean	178.128.161.139 – US – Digital Ocean
137.184.239.50 – US – Digital Ocean	164.92.100.80 – US – Digital Ocean	178.128.166.143 – UK – Digital Ocean
137.184.60.207 – US – Digital Ocean	164.92.105.69 – US – Digital Ocean	178.128.168.229 – UK – Digital Ocean
138.197.140.158 – CA – Digital Ocean	164.92.113.78 – US – Digital Ocean	204.48.29.243 – US – Digital Ocean
138.68.128.55 – UK – Digital Ocean	164.92.120.231 – US – Digital Ocean	206.189.119.217 – UK – Digital Ocean
138.68.163.72 – UK – Digital Ocean	164.92.120.236 – US – Digital Ocean	209.97.186.31 – UK – Digital Ocean
138.68.186.112 – UK – Digital Ocean	164.92.120.246 – US – Digital Ocean	68.183.147.115 – US – Digital Ocean
142.93.50.86 – US – Digital Ocean	164.92.69.194 – US – Digital Ocean	68.183.152.205 – US – Digital Ocean
143.198.165.222 – US – Digital Ocean	164.92.70.253 – US – Digital Ocean	

Appendix B – IPs Executing Directory Transversal Attacks

IP address – Country of origin – Hosting provider

102.23.96.17 -- Nigeria—O'Play Digital Services	141.0.8.112 -- Singapore—Opera Software AS	167.99.171.106 -- US—Digital Ocean
102.23.98.13 -- Nigeria—O'Play Digital Services	141.0.9.234 -- Singapore—Opera Norway AS	167.99.54.225 -- US—Digital Ocean
104.131.56.45 -- US—Rock Solid Internet & Telephone	141.0.9.37 -- Singapore—Opera Software	167.99.57.137 -- US—Digital Ocean
104.131.56.48 -- US—Digital Ocean	142.44.136.207 -- Canada—OVH Hosting Inc	167.99.59.72 -- US—Digital Ocean
104.131.56.73 -- US—Digital Ocean	142.93.50.86 -- US—Digital Ocean	17.121.115.30 -- US – Apple
104.131.56.93 -- US – Digital Ocean	143.198.165.222 -- US – Digital Ocean	172.22.1.25 -- NA
104.248.239.181 -- US – Digital Ocean	14.45.218.228 -- Korea – KT Corporation	173.252.83.19 -- US -- Facebook
107.167.107.19 -- US – Opera Software Americas	152.228.166.33 -- France – OVH SAS	173.252.83.3 -- US -- Facebook
107.167.107.241 -- US – Opera Software Americas	157.245.130.211 -- US – Digital Ocean	178.128.149.201 -- US – Digital Ocean
107.167.107.247 -- US – Opera Software Americas	158.69.246.54 -- Canada – OVH Hosting	178.128.157.246 -- US – Digital Ocean
107.167.107.5 -- US – Opera Software Americas	159.223.132.96 -- US – Digital Ocean	178.128.161.139 -- UK – Digital Ocean
107.167.108.23 -- US – Opera Software Americas	159.223.164.233 -- US – Digital Ocean	178.128.166.143 -- UK – Digital Ocean
107.167.108.60 -- UK – Digital Ocean	159.223.204.244 -- US – Digital Ocean	178.128.168.229 -- UK – Digital Ocean
107.167.109.158 -- US – Opera Software Americas	159.89.128.200 -- US – Digital Ocean	179.60.149.123 -- Nicaragua -- Safe VPN S.A.
107.167.109.165 -- US – Opera Software Americas	159.89.129.171 -- US – Digital Ocean	18.206.199.142 -- US – Amazon Technologies
107.167.109.166 -- US – Opera Software Americas	161.35.48.16 -- US – Digital Ocean	182.135.116.122 -- China – ChinaNet Sichuan Province Network

107.167.109.92 -- US – Opera Software Americas	162.255.116.17 -- US – Namecheap	192.99.100.210 -- Canada – OVH Hosting
107.167.109.93 -- US – Opera Software Americas	164.92.100.60 -- US – Digital Ocean	192.99.37.132 -- Canada – OVH Hosting
107.167.109.98 -- US – Opera Software Americas	164.92.100.61 -- US – Digital Ocean	193.142.146.138 -- Netherlands -- HostSlick
135.181.135.36 -- Finland – Hetzner Online GmbH	164.92.100.80 -- US – Digital Ocean	198.54.114.29 -- US -- Namecheap
137.184.10.255 -- US – Digital Ocean	164.92.105.69 -- US – Digital Ocean	198.54.121.131 -- US -- Namecheap
137.184.116.128 -- US – Digital Ocean	164.92.113.78 -- US – Digital Ocean	199.16.157.180 -- US -- Twitter
137.184.239.50 -- US – Digital Ocean	164.92.120.231 -- US – Digital Ocean	199.16.157.181 -- US -- Twitter
137.184.60.207 -- US – Digital Ocean	164.92.120.236 -- US – Digital Ocean	199.21.113.77 -- US -- ColoCrossing
138.197.140.158 -- Canada – Digital Ocean	164.92.120.246 -- US – Digital Ocean	199.59.150.181 -- US -- Twitter
138.68.128.55 -- UK – Digital Ocean	164.92.69.194 -- US – Digital Ocean	2001:41d0:1004:60b::
138.68.163.72 -- UK – Digital Ocean	164.92.70.253 -- US – Digital Ocean	20.108.172.215 -- UK – Microsoft Corporation
138.68.186.112 -- UK – Digital Ocean	164.92.92.51 -- US – Digital Ocean	20.108.18.12 -- UK – Microsoft Corporation
139.60.161.56 -- US – Hostkey	164.92.98.1 -- US – Digital Ocean	20.117.158.160 -- UK – Microsoft Corporation
20.151.233.207 -- Canada – Microsoft Corporation	2a03:2880:22ff:12::face:b00c	2a03:2880:ff:75::face:b00c
20.205.142.197 -- Hong Kong – Microsoft Corp	2a03:2880:22ff:13::face:b00c	2a03:2880:ff:76::face:b00c
20.222.117.125 -- Japan – Microsoft Corp	2a03:2880:22ff:5::face:b00c	3.216.36.192 -- US – Amazon Data Services NoVa
20.254.151.249 -- UK – Microsoft Corp	2a03:2880:22ff:74::face:b00c	3.237.199.191 -- US – Amazon Data Services NoVa
204.48.29.243 -- US – Digital Ocean	2a03:2880:22ff:75::face:b00c	3.237.76.170 -- US – Amazon Data Services NoVa

206.189.119.217 -- UK – Digital Ocean	2a03:2880:22ff:76::face:b00c	3.238.44.255 -- US – Amazon Data Services NoVa
207.46.13.104 -- US – Microsoft Corp	51.15.164.30 -- France – Scaleway	68.183.147.115 -- US – Digital Ocean
207.46.13.136 -- US – Microsoft Corp	51.79.77.176 -- Canada – OVH Hosting	68.183.152.205 -- US – Digital Ocean
20.90.82.142 -- UK – Microsoft Corp	52.41.129.71 -- US – Amazon Technologies	64.124.8.30 -- US – Castle Global
209.188.31.27 -- US – Namecheap	54.147.246.36 -- US – Amazon Data Services NoVa	76.186.65.238 -- US – Charter Communications
209.94.137.128 -- US – RCN	54.200.17.95 -- US – Amazon	77.234.46.220 -- US – AVAST Software
209.97.135.164 -- UK – Digital Ocean	54.214.215.141 -- US -- Amazon	82.145.223.145 -- Netherlands – Opera Norway AS
209.97.186.31 -- UK – Digital Ocean	54.37.235.123 -- Poland – OVH SAS	83.136.252.73 -- UK – UpCloud
216.168.59.164 -- US – Digital Fortress	54.39.104.161 -- Canada – OVH Hosting	94.130.167.96 -- Germany – Hetzner Online
3.239.45.78 -- US – Amazon Data Services NoVa	64.124.8.36 -- US – Castle Global	76.186.65.238 -- US – Charter Communications
34.229.6.152 -- US – Amazon Technologies	65.108.110.227 -- Finland – Hetzner Online	51.142.233.49 -- UK -- Microsoft
35.236.215.231 -- US – Google	65.108.143.154 -- Finland – Hetzner Online	2600:100c:b238:10ca:2450:671:4a23:a1af – NA
35.240.26.48 -- Belgium – Google	65.108.64.210 -- Finland – Hetzner Online	2607:4000:200:e:1001::8d – US – Univ of WA
35.88.237.249 -- US – Amazon	65.108.73.116 -- Finland – Hetzner Online	2607:fb90:44ba:ef59:792c:be79:fd3a:7a89 – US – T-mobile
3.89.119.108 -- US – Amazon Data Services NoVa	65.108.73.118 -- Finland – Hetzner Online	2607:fb90:8a27:895b:258d:d012:9657:9d43 – US – T-mobile
3.91.194.240 -- US – Amazon Data Services NoVa	65.21.197.27 -- Finland – Hetzner Online	2a01:4f8:121:4076::2 – GER – igrology.ru
40.77.167.44 -- US – Microsoft Corp	66.249.79.118 -- US – Google	2a01:4f8:13a:1f0a::2 – GER – Hetzner.de
51.142.110.123 -- UK – Microsoft	66.249.79.120 -- US – Google	2a01:4f8:190:442a::2 – GER – Hetzner.de

51.142.115.217 -- UK – Microsoft	66.29.129.200 -- US – Namecheap	2a03:2880:13ff:2::face:b00c – US – Facebook search engine
2a03:2880:13ff:75::face:b00c – US – Facebook search engine	2a03:2880:21ff:13::face:b00c – US – Facebook search engine	2a03:2880:25ff::face:b00c – US – Facebook search engine
2a03:2880:21ff:18::face:b00c – US – Facebook search engine	2a03:2880:22ff:9::face:b00c – US – Facebook search engine	2a03:2880:27ff:11::face:b00c– US – fbsv.net
2a03:2880:21ff:6::face:b00c – US – Facebook search engine	2a03:2880:22ff:f::face:b00c – US – Facebook search engine	2a03:2880:27ff:17::face:b00c – US – fbsv.net
2a03:2880:22ff:11::face:b00c – US – Facebook search engine	2a03:2880:24ff:74::face:b00c – US – fbsv.net	2a03:2880:27ff::face:b00c – US – fbsv.net
2a03:2880:ff:1e::face:b00c – US – Facebook search engine	2a03:2880:24ff:75::face:b00c – US – fbsv.net	2a03:2880:2ff:1::face:b00c – US – Facebook search engine
2a03:2880:ff:5::face:b00c – US – Facebook search engine	2a03:2880:24ff::face:b00c – US – fbsv.net	2a03:2880:31ff:4::face:b00c – Ireland – fbsv.net
2a03:2880:ff:6::face:b00c – US – Facebook search engine	2a03:2880:25ff:1d::face:b00c – US – Facebook search engine	2a03:2880:31ff:74::face:b00c – Ireland – fbsv.net
2a03:2880:ff:75::face:b00c – US – Facebook search engine	2a03:2880:25ff:3::face:b00c – US – Facebook search engine	2a03:2880:31ff:b::face:b00c – Ireland – fbsv.net
2a03:2880:ff:76::face:b00c – US – Facebook search engine	2a03:2880:25ff:4::face:b00c – US – Facebook search engine	2a03:2880:ff:11::face:b00c – US – Facebook search engine
2a03:2880:20ff:9::face:b00c – US – fbsv.net	2a03:2880:25ff:74::face:b00c – US – Facebook search engine	2a03:2880:ff:14::face:b00c – US – Facebook search engine

Appendix C – IPs that Failed to Upload a Web Shell

105.158.17.217 – Morocco – Maroc Telecom