CEOIndustries, Inc.

# Penetration Test Report

Critical Role Productions, LLC

September 25, 2023


**Critical Role Productions, LLC**

3727 W Magnolia Blvd.
#817
Burbank, CA 91505
United States of America

Tel: 1-913-649-1364
Email: info@critrole.com
Web: https://critrole.com

## Table of Contents

# Executive Summary and Overview

CEOIndustries, Inc. ("CEOIndustries") was contracted by Critical Role Productions, LLC ("Critical Role") to conduct a black-box penetration test in order to determine the company's potential exposure to a targeted attack. Critical Role is a multimedia entertainment production company incorporated in 2015 by the members of the creator-owned streaming shows. The main streaming show is a weekly livestream that uses roleplaying game mechanics to explore and develop stories designed to provide an exciting escape from reality and change reality for the better. Critical Role is committed to ensuring that their produced content maintains its confidentiality, integrity, and availability.

All activities were conducted in a manner that simulated a malicious actor engaged in the beginning stages of reconnaissance to build up an attack against Critical Role with the goals of:

- Assessing the ability of a remote attacker to penetrate Critical Role's defenses simply by searching publicly available information with no internal knowledge of Critical Role's systems or architecture.
- Determining the likelihood of a security breach based on the types and amount of information a passive actor could obtain, including:
    - Confidential and Personally Identifiable Information (PII) such as trade secrets, financial information, or confidential assets
    - Internal infrastructure and vulnerabilities of Critical Role's information systems

Efforts were placed on the identification and exploitation of security weaknesses that could allow a remote attacker to gain unauthorized access to organizational data. The attacks were conducted with the level of access that a general Internet user would have. The assessment was conducted in accordance with the recommendations outlined in NIST SP 800-115 (http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf) with all tests and actions being conducted in a passive and nonintrusive manner.

## Summary of Results

Initial reconnaissance of the Critical Role network resulted in mining and accumulating data and information specific to Critical Role and its Internet resources. The results provided us with a vast amount of data that could potentially be used in future, more active and intrusive, stages of pentesting for the company. An examination of Critical Role's main website led to accessible corporate information such as its business registration, subsidiaries, affiliates, trademark filings, etc. After creating a list identifying such entities and associations, it was simple to delve deeper to obtain information regarding the company's business operations.

An examination of the business operations then gave us access to a list of executives and employees, along with their pictures, titles, roles, active social media accounts, and a host of other information. After a closer examination, we determined that despite possessing so much information about the company and its employees, because Critical Role does not own its IP domain (having two IP addresses) or DNS server, there is not a huge risk of an actor gaining access to the company's internal network at this stage. Social engineering and active attacks such as SQL injections, brute force password attempts, and perhaps physical access to the headquarters would be needed to determine the true security of the network and security systems.

**We recommend additional, active black-box testing as well as perhaps a minimal white-box assessment, in order to identify any vulnerabilities that could be taken advantage of at the next level of attacks/testing.**

# Attack Narrative

## Footprinting With Google

For the purposes of this assessment, Critical Role provided minimal information outside of the organizational domain name: critrole.com. The intent was to closely simulate an adversary without any internal information. To avoid targeting systems that were both owned and not owned by Critical Role, there were no active attacks conducted.

In an attempt to gather as much information as possible to identify the potential attack surface, we first examine Critical Role's website: https://critrole.com. By using both simple and advanced Google searches with operators I was able to gather the necessary basic company information needed to proceed with a more active attack. Resources and tools used have been listed in Appendix A – Resources.

### Incorporation and Business Structure:

| | |
|---|---|
| **Main Company:** | **Critical Role Productions, LLC (alias "Critical Role")**<br>**Status:** Active and in Good Standing<br>**Incorporated In**: 2015<br>**State of Incorporation**: California, USA<br>**Type:** Privately Held Limited Liability Company<br>**Headquarters Address:** 3727 W Magnolia Blvd #817, Burbank, CA 91505<br>**Number of Employees:** Approximately 40<br>**Website:** https://critrole.com |
| **Other Subsidiaries/Affiliates:** | **Critical Role Foundation**<br>**Status:** Active and in Good Standing<br>**TaxID:** 82-2787844<br>**Incorporated In:** 2019<br>**State of Incorporation:** Delaware, USA<br>**Type:** 501(c)3 Nonprofit Organization<br>**Headquarters Address:** 2025 North Lincoln Street, Burbank, CA 91504<br>**Email:** info@criticalrolefoundation.org |
| | **Critical Role LLC**<br>**Status:** Active and in Good Standing<br>**Incorporated In:** 2020<br>**State of Incorporation:** California, USA<br>**Type:** Privately Held Limited Liability Company<br>**Key Principle:** Kyle Shire<br>**Headquarters Address:** 2025 North Lincoln Street, Burbank, CA 91504 |

| | |
|---|---|
| | **Darrington Press LLC**<br>**Status:** Active and in Good Standing<br>**Incorporated In:** 2020<br>**State of Incorporation:** California, USA<br>**Type:** Privately Held Limited Liability Company<br>**Key Principles:** Ivan Van Norman and Matthew Mercer<br>**Headquarters Address:** 2025 North Lincoln Street, Burbank, CA 91504 |
| | **CR Real Estate Holdings LLC**<br>**Status:** Active and in Good Standing<br>**Incorporated In:** 2022<br>**State of Incorporation:** California, USA<br>**Type:** Privately Held Limited Liability Company<br>**Headquarters Address:** 2025 North Lincoln Street, Burbank, CA 91504 |
| **Executives and Employees:** | **- Liam O'Brien → co-founder, cast member, executive producer of The Legend of Vox Machina animated series on Amazon Prime**<br>**- Marisha Ray → Creative Director, cast member, executive producer of The Legend of Vox Machina animated series on Amazon Prime**<br>**- Sam Riegel → co-founder, cast member, executive producer of The Legend of Vox Machina animated series on Amazon Prime**<br>**- Travis Willingham → Chief Executive Officer, cast member, and executive producer of The Legend of Vox Machina animated series on Amazon Prime**<br>**- Taliesin Jaffe → co-founder, cast member, executive producer of The Legend of Vox Machina animated series on Amazon Prime**<br>**- Ashley Johnson → President of the Critical Role Foundation, cast member, and executive producer of The Legend of Vox Machina animated series on Amazon Prime**<br>**- Matthew Mercer → Chief Creative Officer, cast member, and executive producer of The Legend of Vox Machina animated series on Amazon Prime**<br>**- Laura Bailey → co-founder, cast member, and executive producer of The Legend of Vox Machina animated series on Amazon Prime**<br>**- Ed Lopez → Chief Operating Officer acts in the role of (but not named) VP of Strategy and Operations being responsible for product strategy, lifecycle, and P&L for Alpha, subscriptions, content management, usability/beta testing, engineering, and quality assurance**<br>**- Rachel Romero → SVP of Marketing and board member of Critical Role Foundation – consumer marketing,** |

| | |
|---|---|
| | **promotion efforts, large-scale digital content distribution, online/offline events, mobile and OTT apps, and eCommerce, social media marketing campaigns, public relations**<br>**- Ben Van Der Fluit → SVP of Business & Content Development to accelerate growth beyond the screen into new mediums and ventures.**<br>**- Mark Koro → Board member of Critical Role Foundation**<br>**- Aaron Monroy → Art Director**<br>**- Nadia Dilbert → Director, Consumer Products & Project Manager, Soft Lines & Hard Goods**<br>**- Allyson De Simone→ Director, Procurement**<br>**- Brittney Austin → Senior Manager, Marketing**<br>**- Surena Marie → Manager, Marketing & Community**<br>**- Jennifer Veloso → Customer Services Representative**<br>**- Bryn Hubbard → Post Production Coordinator**<br>**- Niki Chi → Online Operations Coordinator**<br>**- Nicole Yonan → Marketing Coordinator**<br>**- Max Schapiro → Editor**<br>**- Jordyn Torrence → Graphic Designer**<br>**- Ashleigh Fell → Senior Project Manager**<br>**- Maxwell James → Senior Producer**<br>**- Ashley Middlebrook → Producer**<br>**- Vinnie Singh → Head of Production**<br>**- Tal Levitas → Supervisor, Post Production**<br>**- Dolores Verdiell → Contract Designer**<br>**- Steven Failows → Producer**<br>**- Dani Carr → Lorekeeper**<br>**- Robert Doig → Agent** |
| **Other Information** | **Public facing sites of interest, such as domains, websites, portals, etc:**<br>They have the following social media accounts:<br>- Facebook<br>- Instagram<br>- Apple Itunes/Podcasts<br>- Linked-In<br>- Pinterest<br>- Twitch |

| | |
|---|---|
| | - Twitter ("X")<br>- Youtube<br>- Spotify<br>- Google Podcasts<br>**Web Technology Spend in 2023:** $25,968 USD/year.<br>**Hired a third-party professional chat moderation service:** to pay, train, and properly support moderation efforts on their Twitch channel.<br>**Trademarks, copyrights, logos:** 8 trademarks found from the United States Patent Trademark Office, under attorney Mark A. Watkins at Vorys, Sater, Seymour and Pease LLP at P.O. Box 2255, Columbus, Ohio 43216. |

## Footprinting with WHOIS and DNS Interrogation

Below, we have provided screenshots of our command line searches using NSLookup, WHOIS, and DNS Interrogation. At the end of this Section, there is a summary of our findings.

### NSLookup for critrole.com:

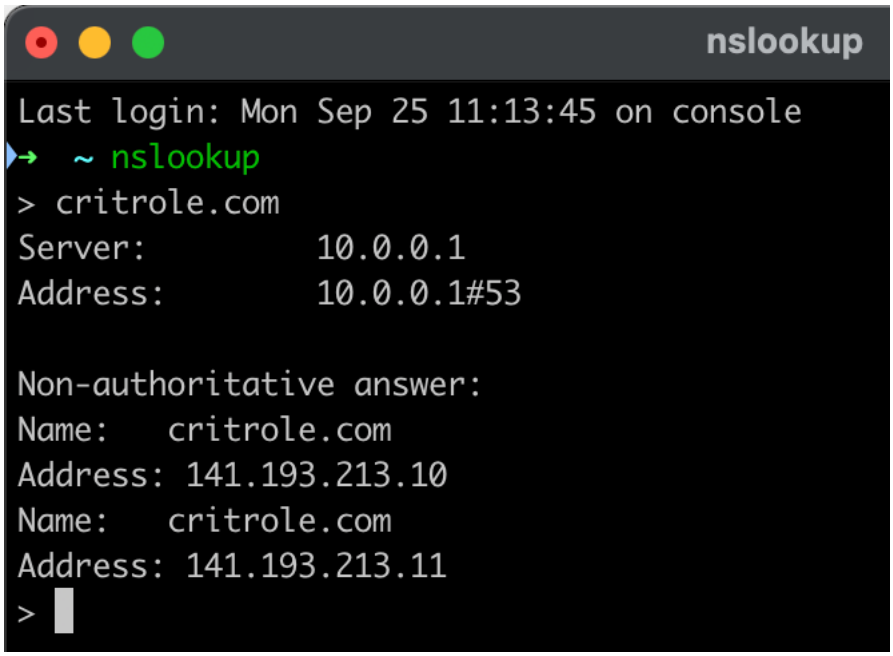


Figure 1 – Information gathering for critrole.com reveals two IP addresses.

## NSLookup Type SOA for critrole.com:

```
> set type=SOA
> critrole.com
Server:         10.0.0.1
Address:        10.0.0.1#53

Non-authoritative answer:
critrole.com
        origin = carter.ns.cloudflare.com
        mail addr = dns.cloudflare.com
        serial = 2307583543
        refresh = 10000
        retry = 2400
        expire = 604800
        minimum = 3600

Authoritative answers can be found from:
> server carter.ns.cloudflare.com
Default server: carter.ns.cloudflare.com
Address: 172.64.33.80#53
Default server: carter.ns.cloudflare.com
Address: 108.162.193.80#53
Default server: carter.ns.cloudflare.com
Address: 173.245.59.80#53
```

Figure 2 – Information gathering for critrole.com reveals Critical Role does not own their domain or DNS server.

```
> server dns.cloudflare.com
Default server: dns.cloudflare.com
Address: 104.16.133.229#53
Default server: dns.cloudflare.com
Address: 104.16.132.229#53
```

Figure 3 – DNS nameserver search confirms the above.

**NSLookup Type A for critrole.com:**

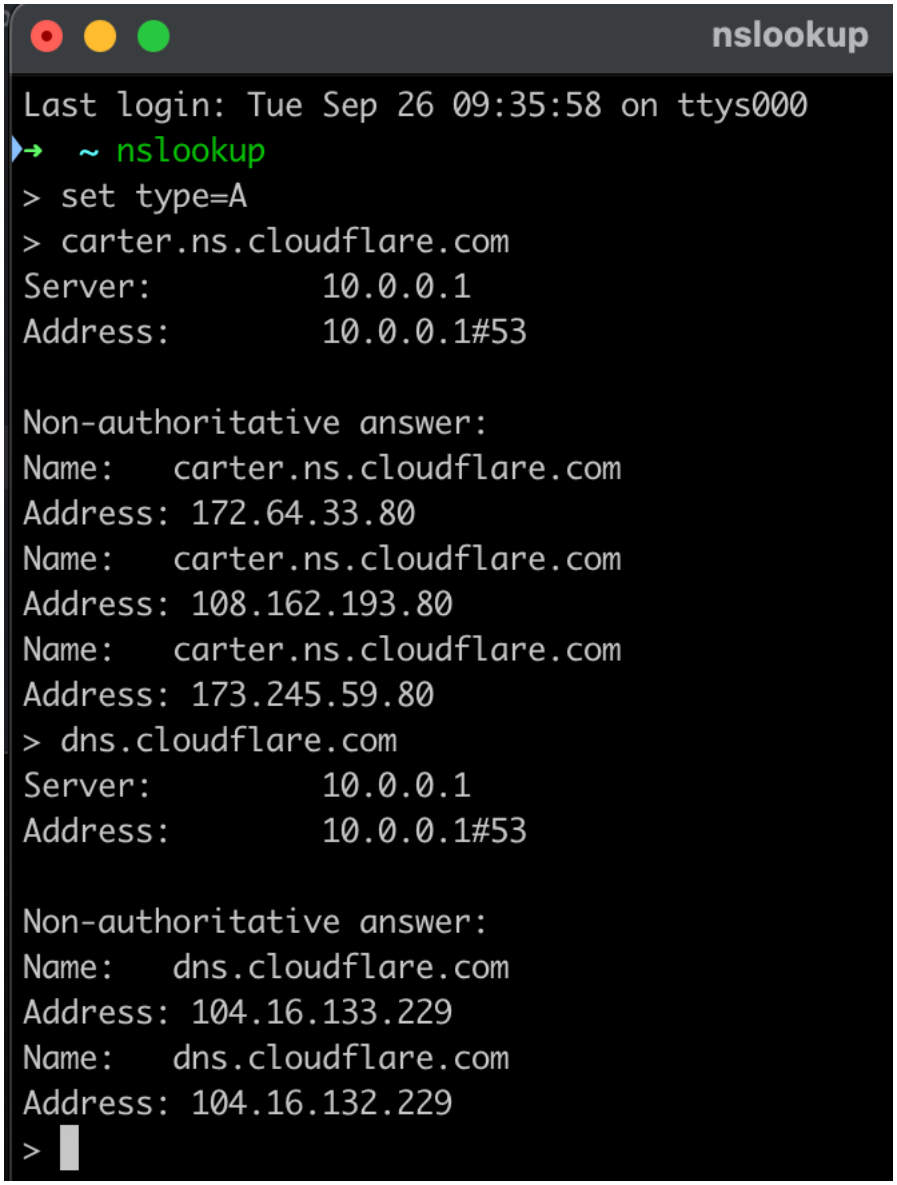


Figure 4 – NSLookup Type A search to confirm.

## Dig +Trace for critrole.com:

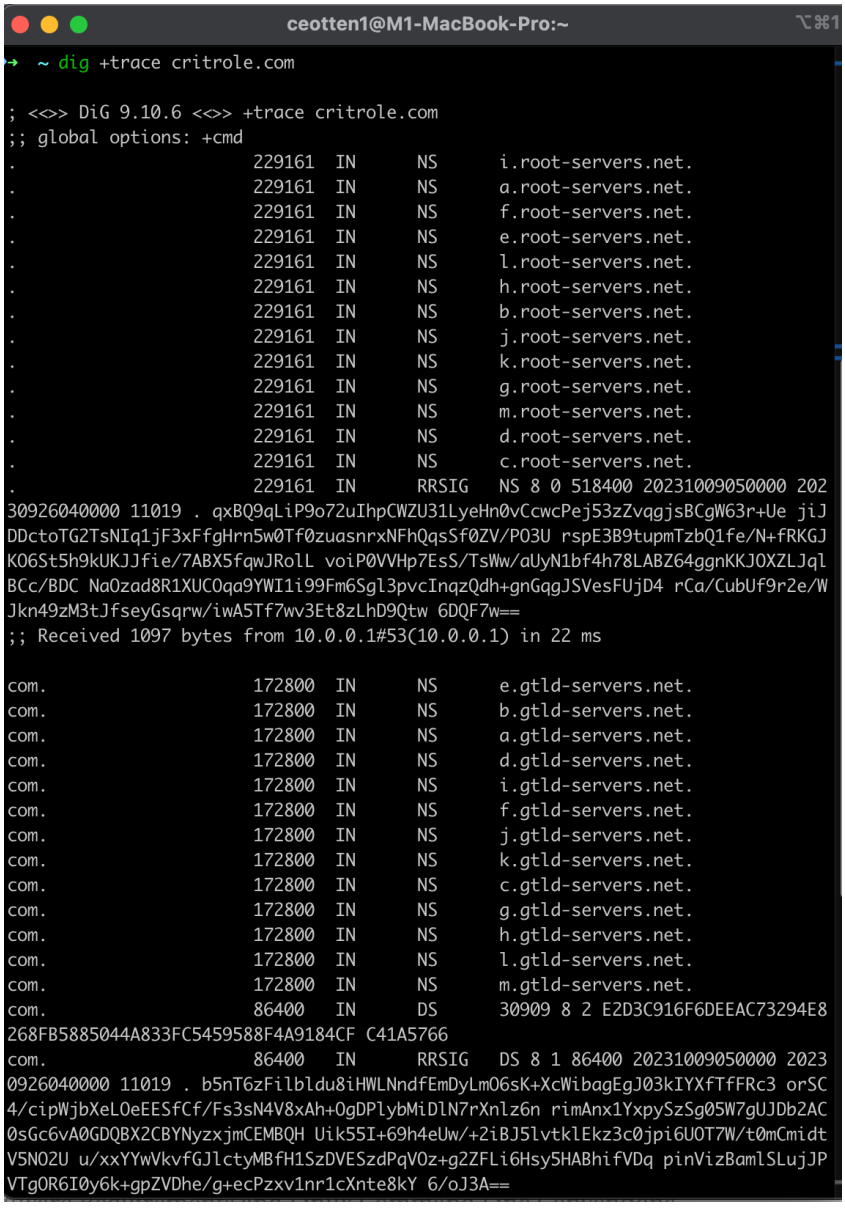


Figure 5 – Dig +Trace search to confirm IP Addresses and lack of ownership.

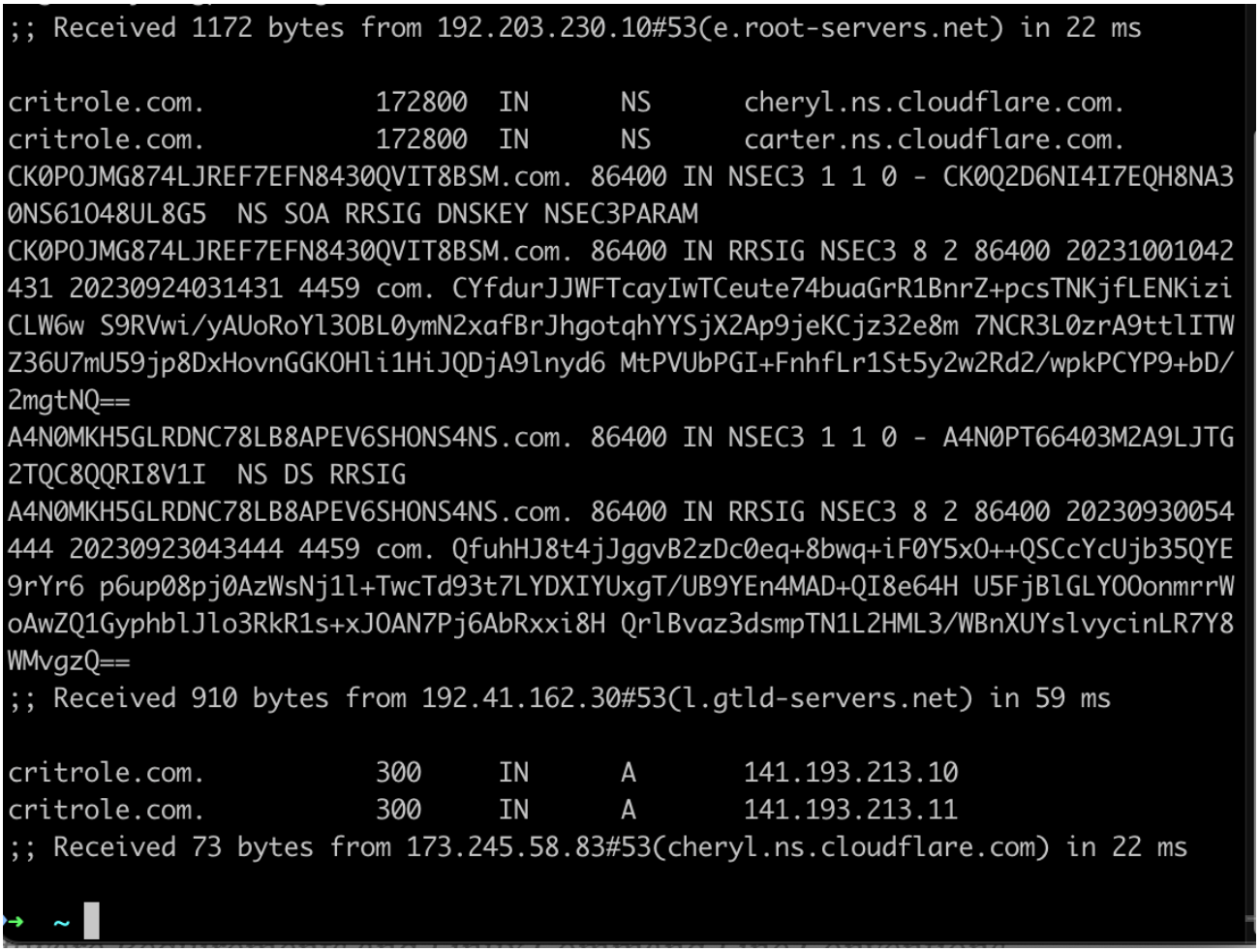


Figure 6 – Cont'd: Dig +Trace search to confirm IP Addresses and lack of ownership.

## NSLookup Type NS for critrole.com:

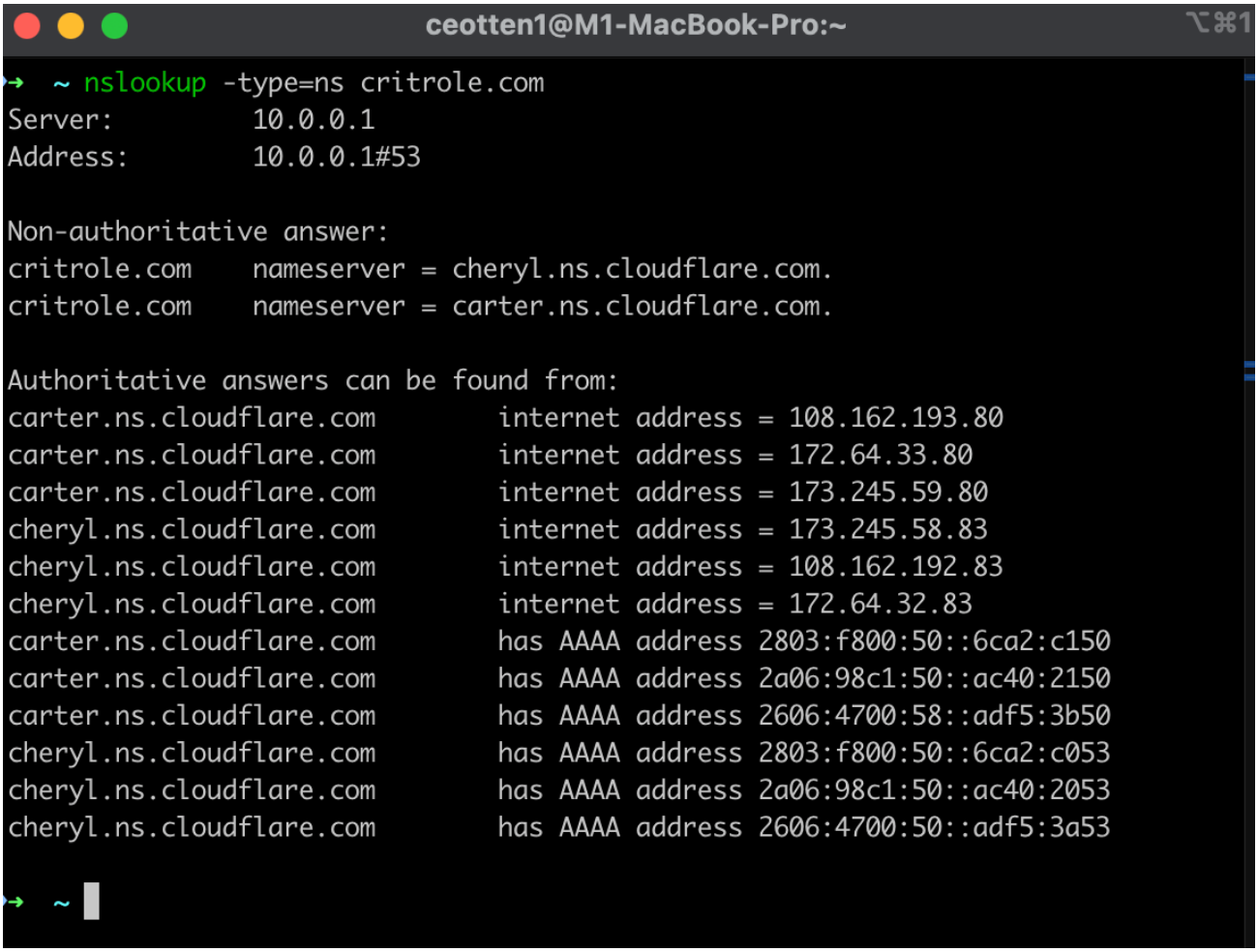


Figure 7 – NSLookup Type NS confirming that the DNS servers are Cheryl and Carter owned by Cloudflare.

## NSLookup Type MX for critrole.com:

```
➜  ~ nslookup -type=mx critrole.com
Server:         10.0.0.1
Address:        10.0.0.1#53

Non-authoritative answer:
critrole.com    mail exchanger = 5 alt1.aspmx.l.google.com.
critrole.com    mail exchanger = 10 alt3.aspmx.l.google.com.
critrole.com    mail exchanger = 5 alt2.aspmx.l.google.com.
critrole.com    mail exchanger = 1 aspmx.l.google.com.
critrole.com    mail exchanger = 10 alt4.aspmx.l.google.com.

Authoritative answers can be found from:
```

Figure 8 – NSLookup Type MX confirming that Critical Role does not own their email server.

## NSLookup Type MX for critrole.com:

```
➜  ~ nslookup
> set type=txt
> critrole.com
Server:         10.0.0.1
Address:        10.0.0.1#53

Non-authoritative answer:
critrole.com    text = "MS=ms83513853"
critrole.com    text = "google-site-verification=W1AeVpCSgjIRTDpaR8stPpjGB1n6oxL3wGSsOJZBWM4"
critrole.com    text = "v=spf1 include:_spf.google.com include:shops.shopify.com include:critrole.com ~all"

Authoritative answers can be found from:
>
```

Figure 9 – NSLookup Type TXT revealing that they use Shopify.

**IP2Location for critrole.com domains 141.193.213.11 (141.193.213.10 not shown):**

IP2LOCATION Home Products Pricing

| | |
|---|---|
| **Permalink** | https://www.ip2location.com/141.193.213.11 |
| **IP Address** | 141.193.213.11 |
| **Country** | United States of America [US] |
| **Region** | Texas |
| **City** | Austin |
| **Coordinates of City** | 30.271158, -97.741701<br>(30°16'16"N 97°44'30"W) |
| **ISP** | WPEngine Inc. |
| **Local Time** | 26 Sep, 2023 10:34 AM (UTC -05:00) |
| **Domain** | wpengine.com |
| **Net Speed** | (T1) Data Center/Transit |
| **IDD & Area Code** | (1) 512 |
| **ZIP Code** | 78701 |
| **Weather Station** | Austin (USTX0057) |
| **Mobile Carrier** | - |
| **Mobile Country Code - MCC** | - |

Figure 10 – IP2Location search reveals the host/owner of Critical Role's website.

| | |
|---|---|
| ☐ **Mobile Network Code - MNC** | - |
| ☐ **Elevation** | 147m |
| ☐ **Usage Type** | (DCH) Data Center/Web Hosting/Transit |
| ☐ **Address Type** | Anycast |
| ☐ **Category** | Technology & Computing |
| ☐ **District** | Travis County |
| ☐ **ASN** | AS209242 CloudFlare London LLC |
| ☐ **Anonymous Proxy** | Yes |
| ☐ **Proxy Type** | PUB |
| ☐ **Proxy ASN** | AS209242 |
| ☐ **Threat** | BOTNET |
| ☐ **Last Seen** | 10 ago |
| ☐ **Provider** | - |
| **Olson Time Zone** | America/Chicago |

**Figure 11 – Cont'd: IP2Location search reveals the host/owner of Critical Role's website.**

## U.S. Patent and Trademark Office Search for Critical Role trademarks:

### Trademark registrations

| MARK TEXT | IMAGE | REGISTER | NICE CLASSIFICATIONS | REGISTRATION DATE | EXPIRY DATE | |
|---|---|---|---|---|---|---|
| MIGHTY NEIN | MIGHTY NEIN | United States Patent and Trademark Office | 21 | 2021-06-01 | | details |
| MIGHTY NEIN | MIGHTY NEIN | United States Patent and Trademark Office | 9, 16, 25, 28, 38, 41 | 2020-12-22 | | details |
| |  | United States Patent and Trademark Office | 16, 25, 28, 41 | 2020-08-25 | | details |
| CRITICAL ROLE | CRITICAL ROLE | United States Patent and Trademark Office | 16, 21, 25, 28, 38, 41 | 2020-08-11 | | details |
| VOX MACHINA | VOX MACHINA | United States Patent and Trademark Office | 9, 16, 21, 25, 28, 38, 41 | 2020-08-11 | | details |
| HOW DO YOU WANT TO DO THIS? | How do you want to do this? | United States Patent and Trademark Office | 25, 41 | 2018-12-04 | | details |
| CRITICAL ROLE |  | United States Patent and Trademark Office | 25, 41 | 2017-08-15 | | details |
| CRITICAL ROLE | CRITICAL ROLE | United States Patent and Trademark Office | 38, 41 | 2016-03-01 | | details |

**Figure 12 – A U.S. Patent search reveals 8 trademarks in the name of Critical Role and their attorney information.**

## NSLookup for criticalrolefoundation.org:

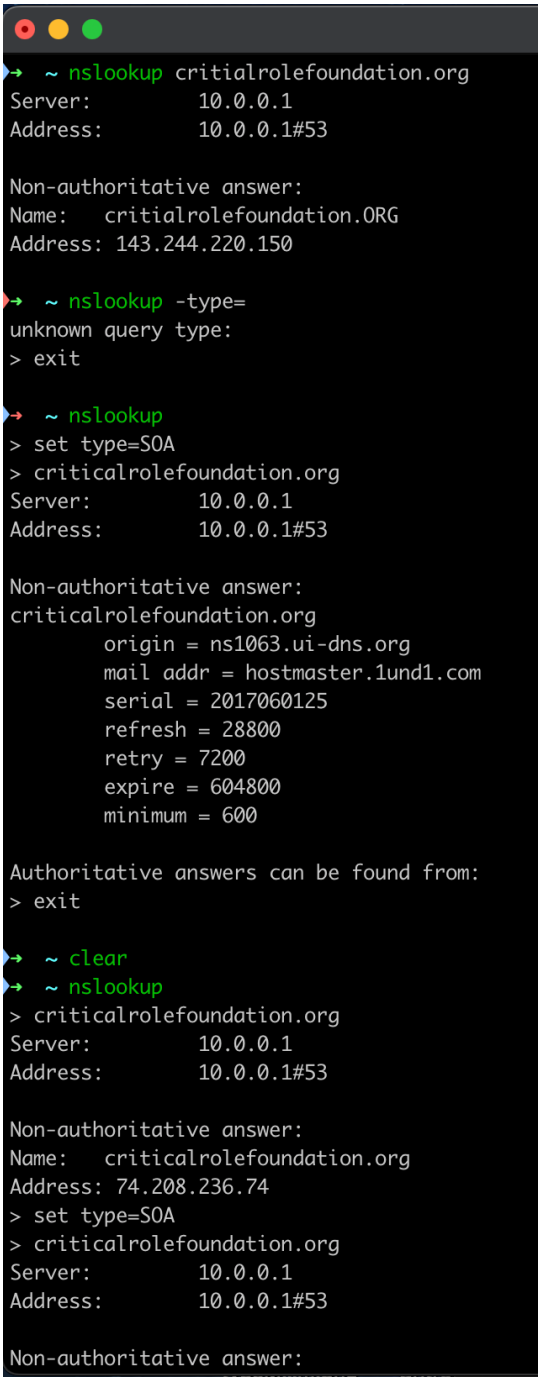


Figure 13 – NSLookup for criticalrolefoundation.org revealing that this domain is owned by 1&1.

## NSLookup for criticalrolefoundation.org – Including Types: SOA, A, TXT and DNS Reverse Lookup:

```
Name:   criticalrolefoundation.org
Address: 74.208.236.74
> set type=SOA
> criticalrolefoundation.org
Server:         10.0.0.1
Address:        10.0.0.1#53

Non-authoritative answer:
criticalrolefoundation.org
        origin = ns1063.ui-dns.org
        mail addr = hostmaster.1und1.com
        serial = 2017060125
        refresh = 28800
        retry = 7200
        expire = 604800
        minimum = 600

Authoritative answers can be found from:
> server ns1063.ui-dns.org
Default server: ns1063.ui-dns.org
Address: 217.160.83.63#53
> set type=A
> criticalrolefoundation.org
Server:         ns1063.ui-dns.org
Address:        217.160.83.63#53

Name:   criticalrolefoundation.org
Address: 74.208.236.74
> set type=txt
> criticalrolefoundation.org
Server:         ns1063.ui-dns.org
Address:        217.160.83.63#53

criticalrolefoundation.org      text = "stripe-verification=72cbd6488fc30b7292a4f9c656803ae5be12201efd04d98107e1d8f
fdeea2897"
criticalrolefoundation.org      text = "google-site-verification=O8NE9hvGjxiJK37W4PEekmsYOFaRrepGr9yWyYdPymw"
> > ns1063.-dns.org
Server:         ns1063.ui-dns.org
Address:        217.160.83.63#53

** server can't find ns1063.ui-dns.org: REFUSED
>
```

Figure 14 – NSLookup revealing Critical Role Foundation does not own the IP domains or DNS servers.

## Dig +Trace for criticalrolefoundation.org:

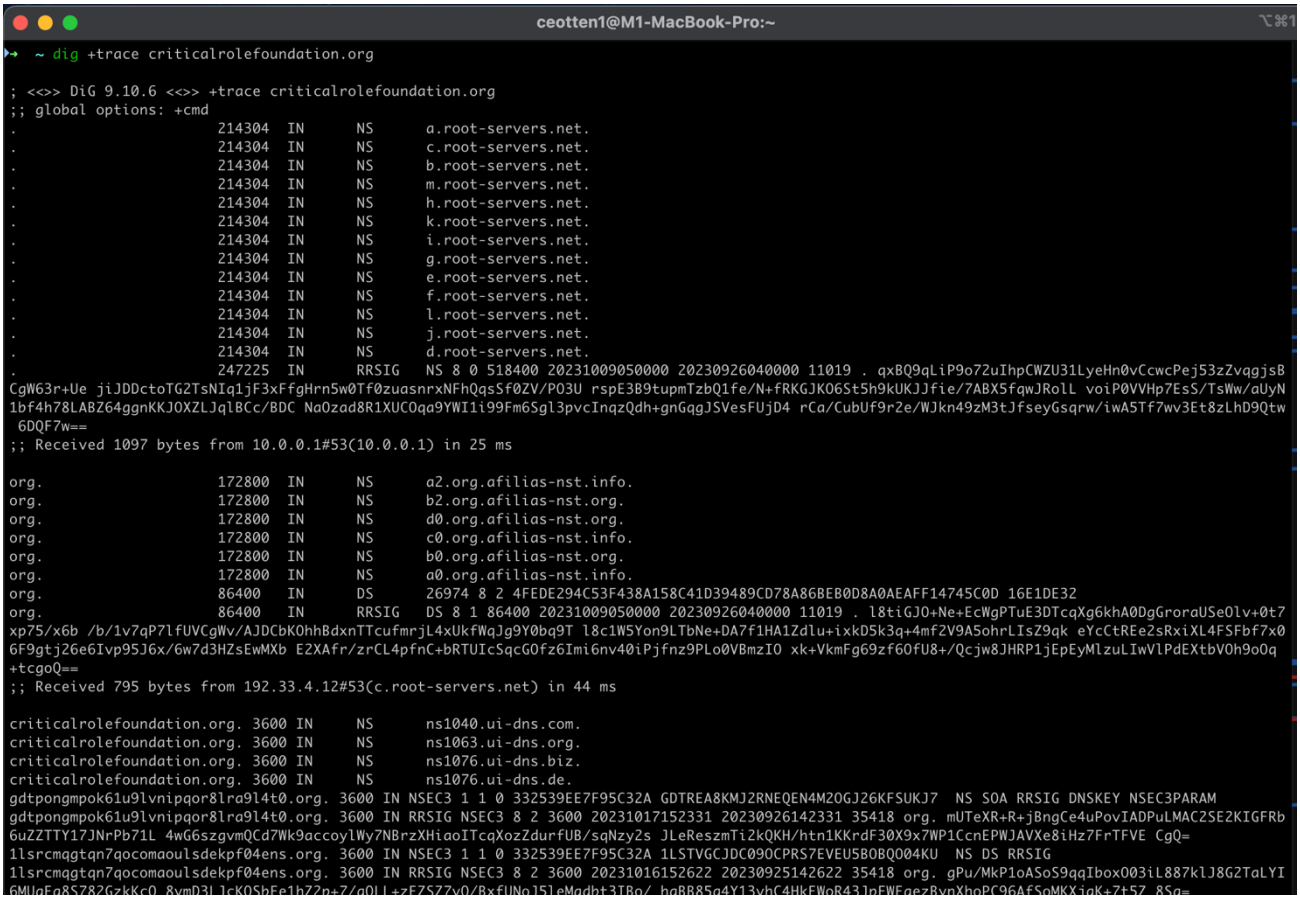


Figure 15 – Dig +Trace Search for criticalrolefoundation.org confirming the NSLookups.

**IP2Location for criticalrolefoundation.org:**

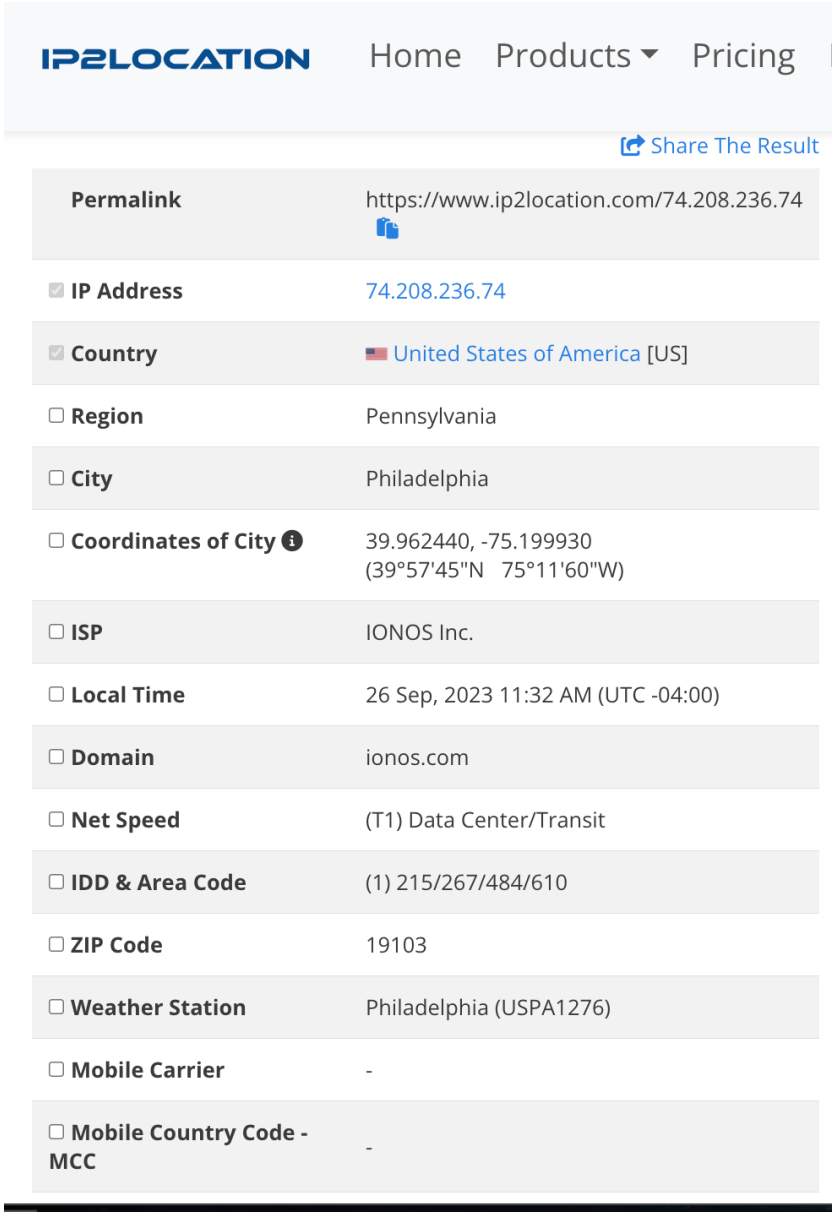


Figure 16 – IP2Location search for Critical Role Foundation IP address revealing it is owned by IONOS.

| | |
|---|---|
| **Elevation** | 15m |
| **Usage Type** | (DCH) Data Center/Web Hosting/Transit |
| **Address Type** | Unicast |
| **Category** | Data Centers |
| **District** | Philadelphia County |
| **ASN** | AS8560 IONOS SE |
| **Anonymous Proxy** | No |
| **Proxy Type** | DCH |
| **Proxy ASN** | - |
| **Threat** | - |
| **Last Seen** | 24 ago |
| **Provider** | - |
| **Olson Time Zone** | America/New_York |

Figure 17 – Cont'd: IP2Location search for Critical Role Foundation IP address revealing it is owned by IONOS.

## Recommendations

Because Critical Role does not own its domain or DNS server we did not perform scanning and were thus unable to build a composite that we feel reflects Critical Role's network.

CEOIndustries recommends that this information be used as the basis for an additional, more active and invasive pentest to more accurately assess Critical Role's security vulnerabilities to a threat from an outside actor. It was determined that while these steps would be possible, they would be considered outside the scope of the current engagement.

CEOIndustries, Inc.

# Appendix A: Resources

- Critrole.com
- Criticalrolefoundation.com
- BuiltWith → builtwith.com
- OpenCorporates → https://opencorporates.com/companies/us_ca/201512810264
- Linked-In → https://www.linkedin.com/company/critical-role
- Dun & Bradstreet, Inc. → www.dnb.com
- California Secretary of State Business → https://bizfileonline.sos.ca.gov/search/business
- U.S. Patent and Trademark Office → https://tsdr.uspto.gov/#caseNumber=86703125&caseSearchType=US_APPLICATION&caseType=DEFAULT&searchType=statusSearch