

# A Simple Approach to Discovering Oyster Backdoor Infrastructure


 [hunt.io/blog/a-simple-approach-to-discovering-oyster-backdoor-infrastructure](https://hunt.io/blog/a-simple-approach-to-discovering-oyster-backdoor-infrastructure)



TABLE OF CONTENTS

## Introduction

Oyster backdoor, also known as Broomstick ([IBM](#)) and CleanUpLoader ([RussianPanda – X](#)), has been linked to malvertising campaigns mimicking popular software. On June 21st, [Rapid7](#) described how attackers disguised the backdoor as a Microsoft Teams installer, targeting unsuspecting users.

The malicious software collects victim information and **sends it to a hard-coded C2 domain** via an HTTP POST request. Malicious server administrators often leave identifiable clues in their infrastructure setup. As defenders and researchers, identifying these unique markers can help us uncover previously unreported IPs and domains.

In this post, we will examine the Oyster backdoor infrastructure, focusing on HTML titles, body hashes, and TLS certificates.

## Domains Identified by Rapid7

---

In their blog post, Rapid7 identified three domains, the malicious DLLs, CleanUp30.dll and CleanUp.dll, attempted to communicate with:

- **supfoundrysettlers[.]us** IP: 64.95.10[.]243
- **wherehomebe[.]com** IP: 149.248.79[.]62
- **retdirectyourman[.]eu** IP: 206.166.251[.]114

Using this information, we can analyze the above IPs and domains for any anomalies that would assist in developing a query to find additional C2 servers. We will start with the first IP, 64.95.10[.]243, and see what can be found in Hunt.

## Infrastructure Analysis

---

Hunt identified two open ports (22 and 443) on 64.95.10[.]243. Analyzing the HTML response for port 443, depicted in Figure 1, reveals a webpage with the title and content of 'Soon.'

While the simplicity of this webpage does not overtly indicate malicious activity, we will note this finding and proceed to investigate the TLS history for further insights.

```
{
  timestamp : 2024-07-17T01:16:25
  seen_first : 2024-03-25T14:38:15
  seen_last : 2024-07-17T01:16:25
  port : 443
  fingerprint : http
  data : Date: Wed, 10 Jul 2024 01:07:39 GMT
  Server: Apache/2.4.52 (Ubuntu)
  Cache-Control: no-cache, private
  Set-Cookie: XSRF-TOKEN=eyJpdiI6ImxkakluU1JRWVhwNkcrTVlEcFNndEE9PSIsInZhbHVlIjoia1RqRTlj
  Set-Cookie: laravel_session=eyJpdiI6I1lkzdCeEhiWHA3a1ZvOGFENU0lcWc9PSIsInZhbHVlIjoiaUxc
  Vary: Accept-Encoding
  Content-Encoding: gzip
  Transfer-Encoding: chunked
  Content-Type: text/html; charset=UTF-8

  <!DOCTYPE html>
  <html lang="en">
    <head>
      <meta charset="utf-8">
      <meta name="viewport" content="width=device-width, initial-scale=1">
      <title>Soon</title>
    </head>
    <body class="font-sans antialiased dark:bg-black dark:text-white/50">
      Soon
    </body>
  </html>

  matches : [ »
    0 : { »
      description : Apache
      parameters : { »
        service.vendor : Apache
        service.product : HTTPD
        service.family : Apache
        service.version : 2.4.52
        service.cpe23 : cpe:/a:apache:http_server:{service.version}
        apache.info : (Ubuntu)
      }
    }
  ]
}
```

Figure 1: Underlined HTML title for 64.95.10[.]243 (Try it [here](#))

An additional screenshot of the above webpage from [urlscanio](#) can be found below.

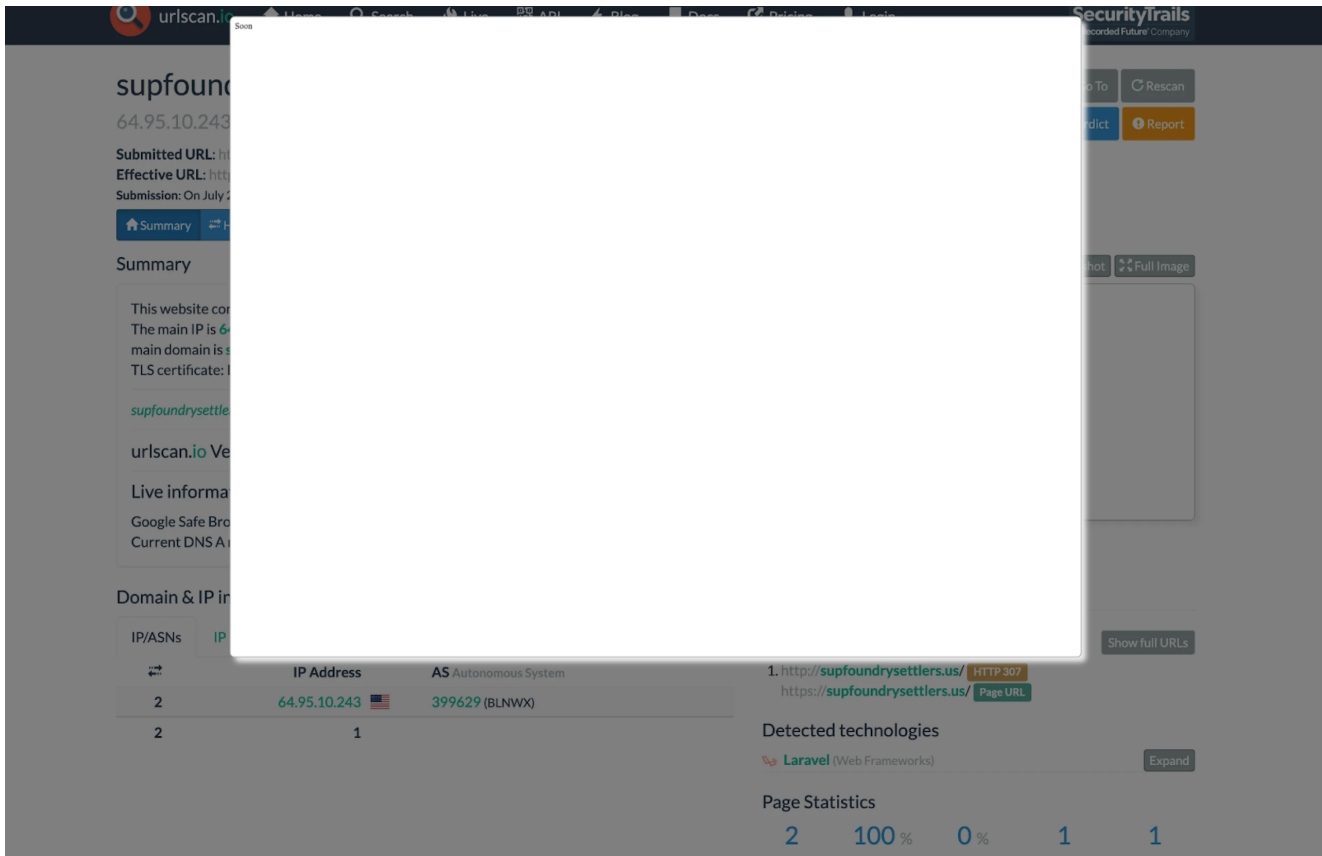


Figure 2: Screenshot of supfoundrysettlers[.]us (Source: [urlscan](https://urlscan.io))

The History tab in Hunt features a time graph that helps identify overlaps in port and certificate activity. Each button is clickable and displays additional information, such as **JA4X**, **JARM hashes**, and **certificate details**.

As shown in Figure 3, the cert's common name matches that of the malicious domain reported in the Rapid7 report, which is still active. Additionally, a JARM hash (the yellow bar at the bottom) will be helpful when crafting our detection query.



## 64.95.10.243 - Overview

Info Domains 1 History (Beta) Associations 2 SSL History SSH History JARM Port History Signals Activity 0

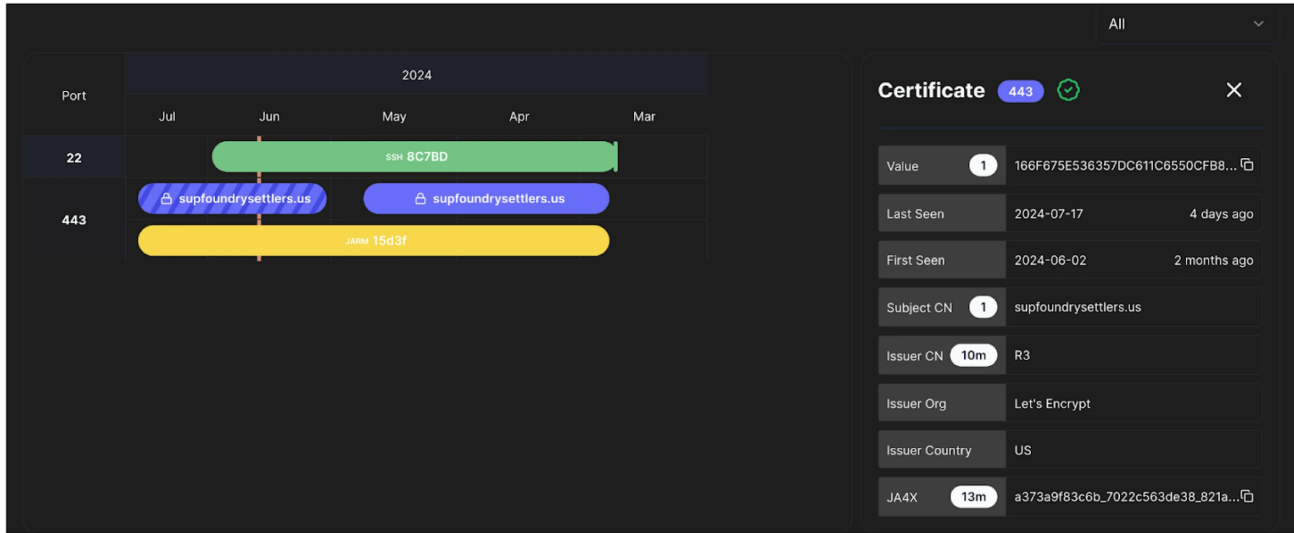


Figure 3: Screenshot of certificate information using the History tab

With no available pivots on port 22, SSH, or other TLS history, it's time to focus on developing a method for identifying the backdoor. Using Let's Encrypt certificates is common practice and would likely result in hundreds of thousands of results alone, but how many web pages have the title 'Soon'?

To understand the prevalence, we'll combine the cert's JARM fingerprint hash with the HTML response body hash. This approach may yield fewer results than searching for specific TLDs using Let's Encrypt.

With that, a pseudocode query to find additional Oyster servers is

```
jarm_fingerprint:"15d3fd16d29d29d00042d43d00000ed1cf37c9a169b41886e27ba8fad60b0"  
AND http_response_hash:"0c90ad9910cfb37c9969e14388707ef765ef5e73"
```

## Our Findings

Our detection rule for locating Oyster infrastructure flagged seven IP addresses, including the three mentioned in the Rapid7 post.

The limited number of results, combined with the already confirmed domain indicators, suggests our query is effective and likely on target until the threat actor decides to change up their C2 TTPs.

Let's Encrypt certificates and ports remained consistent across the returned results, with one exception (193.43.104[.]208), which had ports 80 and 443 open.

A notable difference is the ASNs. The three known domains/IPs were hosted on BL Networks infrastructure, while our findings are hosted on OVH SAS.

Below are the domains we have uncovered, which have a similar naming theme to those mentioned above.

\*Detailed information, including the corresponding IP addresses, can be found at the end of this article.

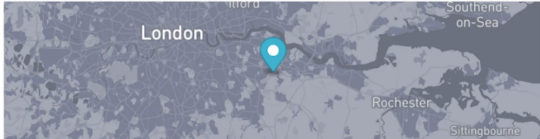
## - codeforprofessionalusers[.]com

### 51.195.232.46 - Overview

Info Domains 1 History (Beta) Associations 0 SSL History SSH History JARM Port History Signals Activity 0

51.195.232.46

OVH Ltd



Bexley, England, GB

**DNS**

Reverse DNS undefined

Forward DNS codeforprofessionalusers.com... 1

Tag

**ASN**

AS16276	51.195.0/16	OVH SAS
---------	-------------	---------

**Open Ports and Software**

Name	Port	Product	Version	Extra Info	Last Seen	First Seen
SSH	22	-	-	-	1 week ago	10 months ago
TLS/HTTP	443	HTTPD	2.4.52	-	3 days ago	3 weeks ago

Figure 4: Overview of suspected Oyster backdoor IP (Check it out [here](#))

## - postmastersoriginals[.]com

# 139.99.221.140 - Overview

Info Domains 1 History (Beta) Associations 0 SSL History SSH History JARM Port History Signals Activity 1

139.99.221.140

OVH Australia PTY LTD

Sydney, New South Wales, AU

### DNS

Reverse DNS undefined

Forward DNS postmastersoriginals.com... 1

Tag

### ASN

AS16276	139.99.128.0/17	OVH SAS
---------	-----------------	---------

### Open Ports and Software

Name	Port	Product	Version	Extra Info	Last Seen	First Seen	
SSH	22	-	-	-	1 week ago	1 year ago	
TLS/HTTP	443	HTTPD	2.4.52	-	2 weeks ago	8 months ago	

Figure 5: Screenshot showing suspicious domain and ports 22, 443 (Check it out [here](#)) - **firstcountryours[.]eu**

# 162.19.237.181 - Overview

Info Domains 1 History (Beta) Associations 0 SSL History SSH History JARM Port History Signals Activity 0

162.19.237.181

OVH GmbH

Frankfurt am Main, Hesse, DE

### DNS

Reverse DNS undefined

Forward DNS firstcountryours.eu... **1**

Tag

### ASN

AS16276 162.19.128.0/17 OVH SAS

### Open Ports and Software

Name	Port	Product	Version	Extra Info	Last Seen	First Seen	
SSH	22	-	-	-	2 weeks ago	1 year ago	
HTTP	443	HTTPD	2.4.52	-	1 day ago	1 year ago	

Figure 6: Overview of 162.19.237[.]181 and firstcountryours[.]eu (Check it out [here](#)) - dotnetisforchildren[.]com

## 193.43.104.208 - Overview

Info Domains 1 History (Beta) Associations 0 SSL History SSH History JARM Port History Signals Activity 0

193.43.104.208

BlueVPS OU

Frankfurt am Main, Hesse, DE

### DNS

Reverse DNS mwka96bj128g6.easyinsurancequotes.net

Forward DNS dotnetisnotforchildren.com... **1**

Tag

### ASN

AS16276 193.43.104.0/24 OVH SAS

### Open Ports and Software

Name	Port	Product	Version	Extra Info	Last Seen First Seen	
HTTP	80	HTTPD	2.4.52	-	2 days ago 1 year ago	
TLS/HTTP	443	HTTPD	2.4.52	-	2 days ago 1 year ago	

Figure 7: Screenshot of 193.43.104[.]208. Note ports 80 & 443 (link [here](#))

To further corroborate our findings associated with the Oyster backdoor, we can analyze the domains using VirusTotal.

It's important to note that a **VirusTotal score of 0 does not necessarily indicate that an IP or domain is benign**; it simply suggests that additional data may be required for a definitive assessment.

Below are the results for codeforprofessionalusers[.]com and postmastersoriginals[.]com.

Notably, CleanUp.dll has been linked to the Oyster backdoor. Furthermore, additional files appear to spoof Microsoft's Defender, potentially indicating a campaign aimed at users seeking antivirus software.

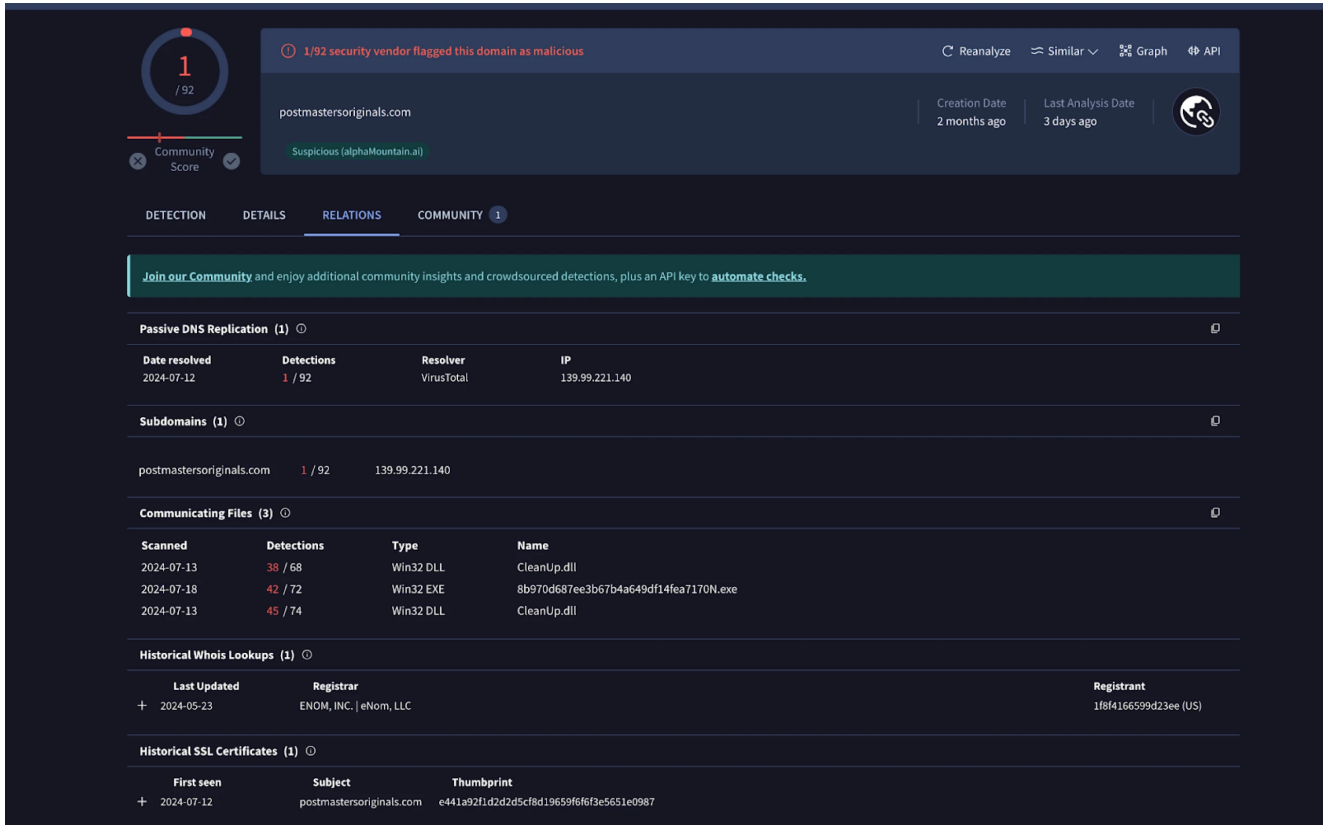


Figure 8: VirusTotal results for postmastersonline.com (Source: [VT](#))

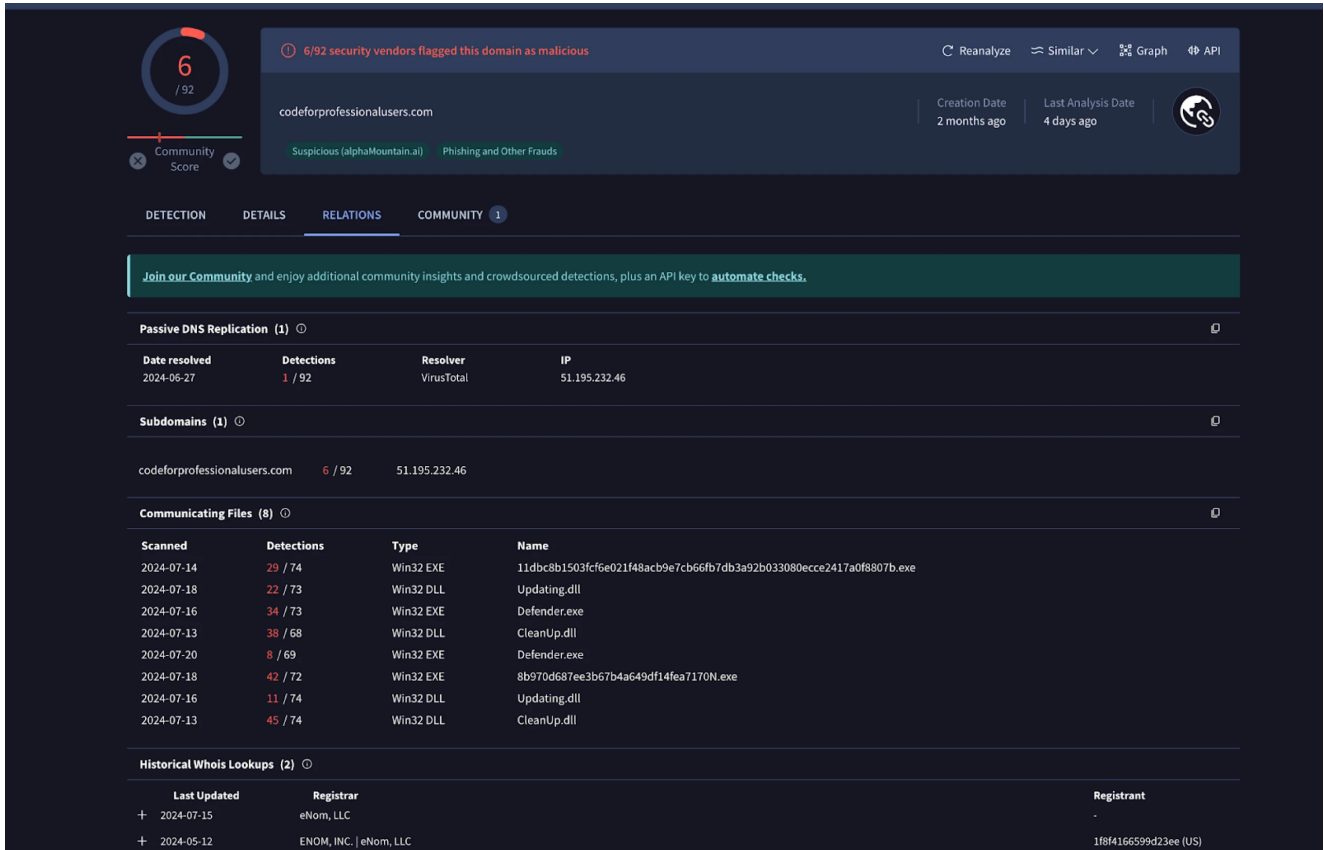


Figure 9: Screenshot of VT results for codeforprofessionalusers.com (Source: [VirusTotal](#))

Digging into any one of the CleanUp.dll files in Figure 10 below reveals a positive detection for the Oyster backdoor and the `/api/connectivity` URL path where victim information is sent via a POST request.

Additionally, under 'Contacted Domains,' we see one of our other finds, `firstcountryours[.]eu` listed.

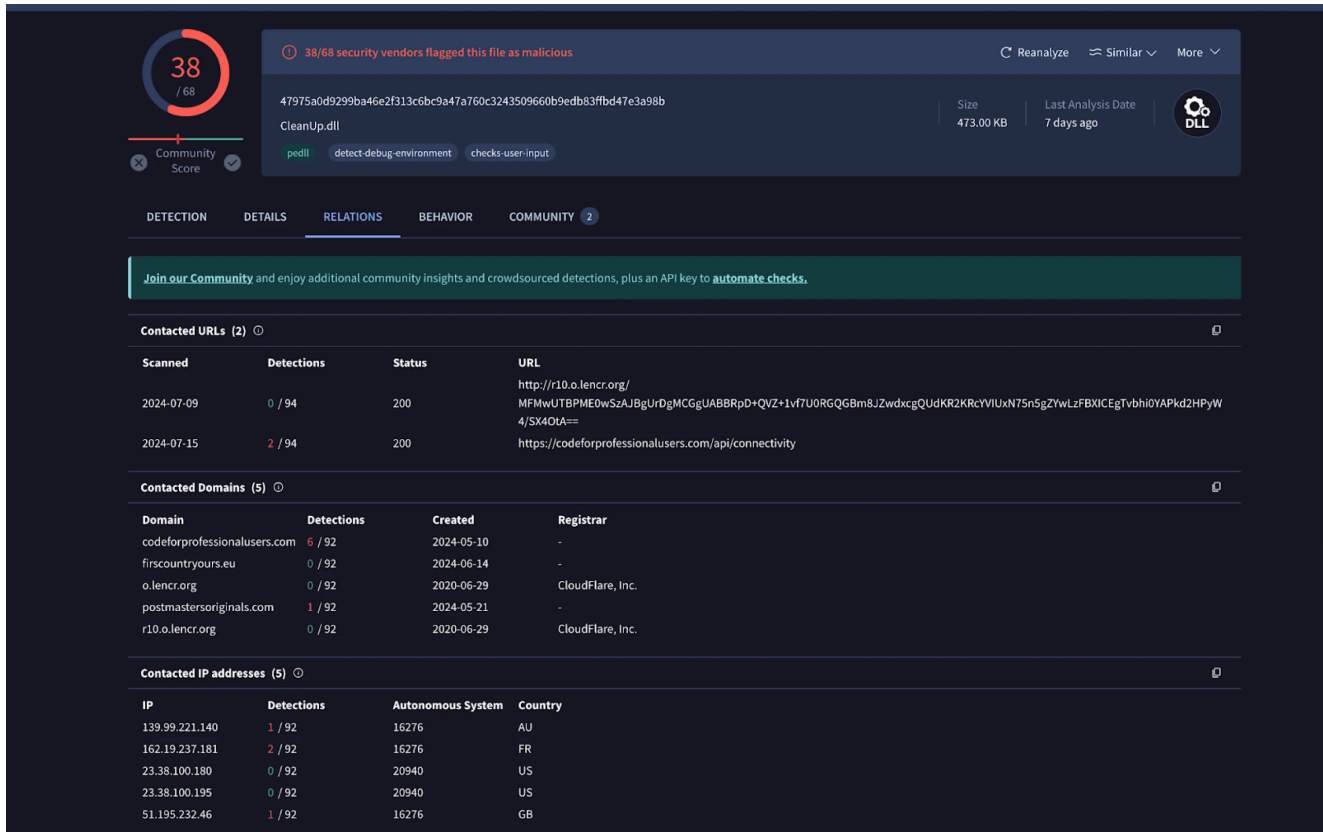


Figure 10: VirusTotal results for contacted URLs and domains of CleanUp.dll (Source: [VT](#))

## Conclusion

We uncovered and validated suspected Oyster backdoor infrastructure with a relatively simple query. While identifying malicious infrastructure can sometimes be straightforward, it's not always this easy and requires thorough analysis and strategic pivots to uncover additional C2s.

If you'd like to see how Hunt can help you expose malicious infrastructure before it's weaponized, contact us to [book a free demo](#) today.

## Network Observables

IP Address	Domain	ANS	Notes
64.95.10[.]243	supfoundrysettlers[.]us	BL Networks	Rapid7 Blog

IP Address	Domain	ANS	Notes
149.248.79[.]62	wherehomebe[.]com	BL Networks	Rapid7 Blog
206.166.251[.]114	retdirectyourman[.]eu	BL Networks	Rapid7 Blog
51.195.232[.]46	codeforprofessionalusers[.]com	OVH SAS	Jarm fingerprint + HTML response hash
139.99.221[.]140	postmastersoriginals[.]com	OVH SAS	Jarm fingerprint + HTML response hash
162.19.237[.]181	firstcountryours[.]eu	OVH SAS	Jarm fingerprint + HTML response hash
193.43.104[.]208	dotnetisforchildren[.]com	OVH SAS	Jarm fingerprint + HTML response hash

## TABLE OF CONTENTS

### Introduction

Oyster backdoor, also known as Broomstick ([IBM](#)) and CleanUpLoader ([RussianPanda – X](#)), has been linked to malvertising campaigns mimicking popular software. On June 21st, [Rapid7](#) described how attackers disguised the backdoor as a Microsoft Teams installer, targeting unsuspecting users.

The malicious software collects victim information and **sends it to a hard-coded C2 domain** via an HTTP POST request. Malicious server administrators often leave identifiable clues in their infrastructure setup. As defenders and researchers, identifying these unique markers can help us uncover previously unreported IPs and domains.

In this post, we will examine the Oyster backdoor infrastructure, focusing on HTML titles, body hashes, and TLS certificates.

### Domains Identified by Rapid7

In their blog post, Rapid7 identified three domains, the malicious DLLs, CleanUp30.dll and CleanUp.dll, attempted to communicate with:

- **supfoundrysettlers[.]us** IP: 64.95.10[.]243
- **wherehomebe[.]com** IP: 149.248.79[.]62
- **retdirectyourman[.]eu** IP: 206.166.251[.]114

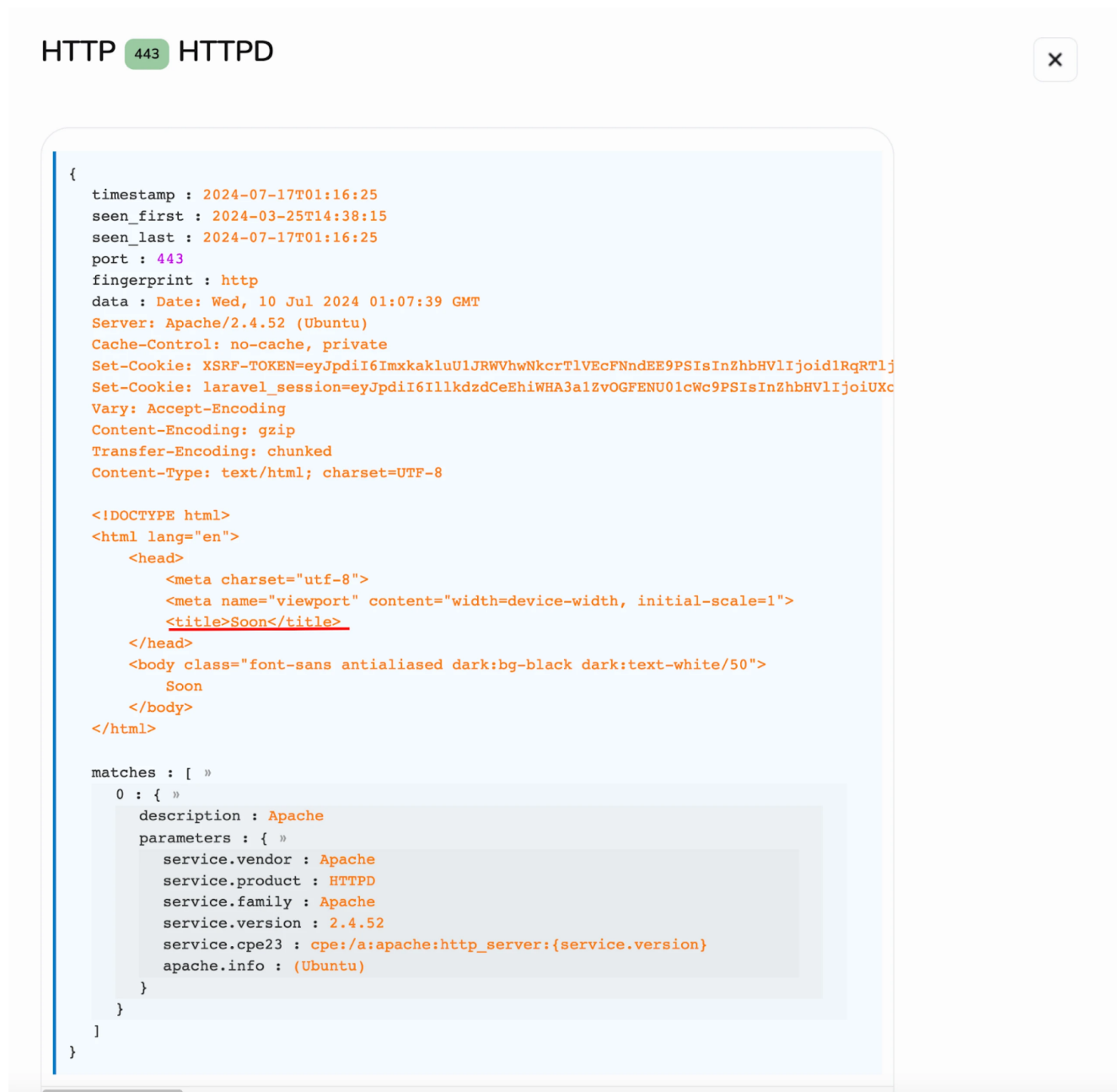


Using this information, we can analyze the above IPs and domains for any anomalies that would assist in developing a query to find additional C2 servers. We will start with the first IP, 64.95.10[.]243, and see what can be found in Hunt.

## Infrastructure Analysis

Hunt identified two open ports (22 and 443) on 64.95.10[.]243. Analyzing the HTML response for port 443, depicted in Figure 1, reveals a webpage with the title and content of ‘Soon.’

While the simplicity of this webpage does not overtly indicate malicious activity, we will note this finding and proceed to investigate the TLS history for further insights.



```
HTTP 443 HTTPD

{
  timestamp : 2024-07-17T01:16:25
  seen_first : 2024-03-25T14:38:15
  seen_last : 2024-07-17T01:16:25
  port : 443
  fingerprint : http
  data : Date: Wed, 10 Jul 2024 01:07:39 GMT
  Server: Apache/2.4.52 (Ubuntu)
  Cache-Control: no-cache, private
  Set-Cookie: XSRF-TOKEN=eyJpdiI6ImxkakluU1JRWHwNkcrTVlVcFNndEE9PSIsInZhbnVlIjojd1RqRTlj
  Set-Cookie: laravel_session=eyJpdiI6I1lkdzdCeEhiWHA3alZvOGFENU0lcWc9PSIsInZhbnVlIjojoiUXc
  Vary: Accept-Encoding
  Content-Encoding: gzip
  Transfer-Encoding: chunked
  Content-Type: text/html; charset=UTF-8

  <!DOCTYPE html>
  <html lang="en">
    <head>
      <meta charset="utf-8">
      <meta name="viewport" content="width=device-width, initial-scale=1">
      <title>Soon</title>
    </head>
    <body class="font-sans antialiased dark:bg-black dark:text-white/50">
      Soon
    </body>
  </html>

  matches : [ »
    0 : { »
      description : Apache
      parameters : { »
        service.vendor : Apache
        service.product : HTTPD
        service.family : Apache
        service.version : 2.4.52
        service.cpe23 : cpe:/a:apache:http_server:{service.version}
        apache.info : (Ubuntu)
      }
    }
  ]
}
```

Figure 1: Underlined HTML title for 64.95.10[.]243 (Try it [here](#))

An additional screenshot of the above webpage from [urlscanio](#) can be found below.

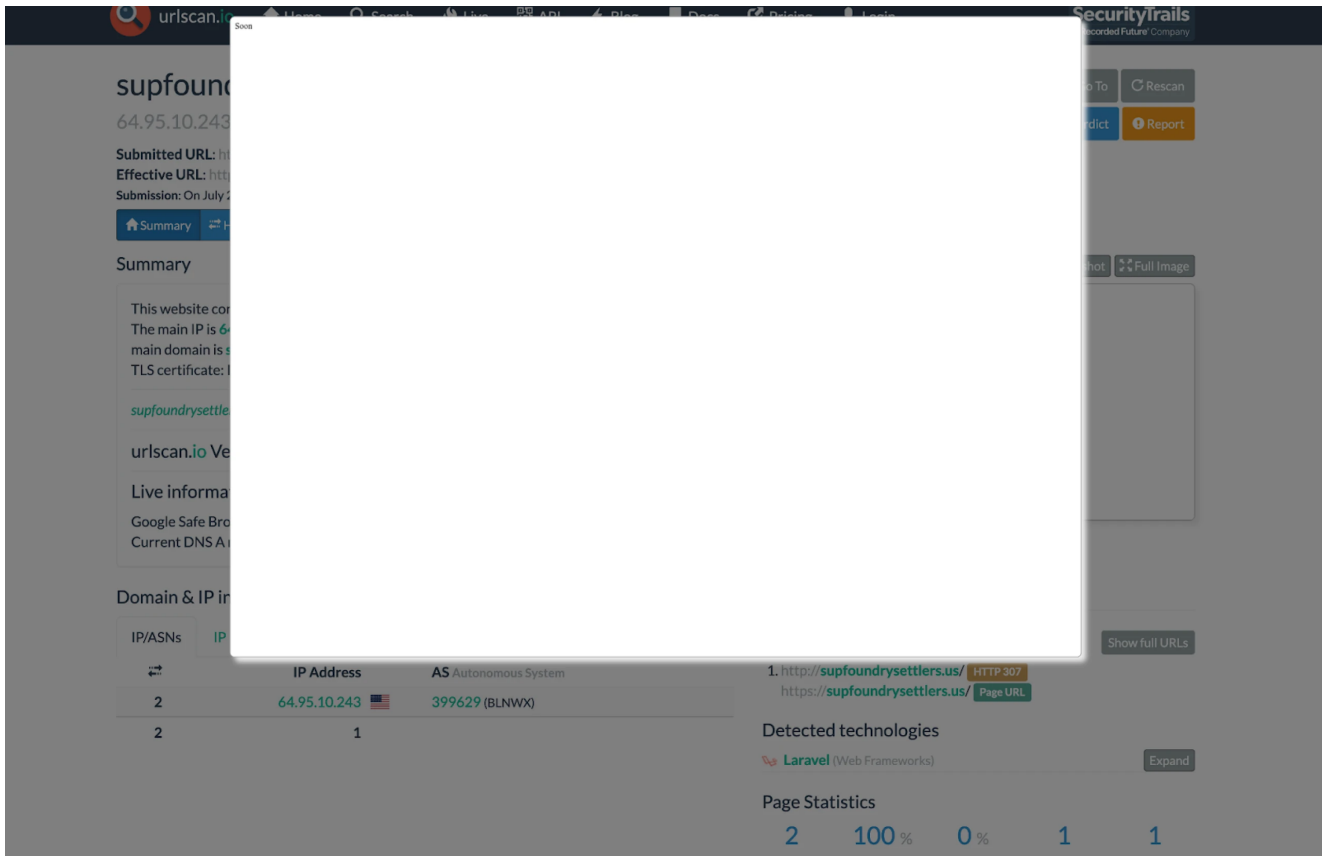


Figure 2: Screenshot of supfoundrysettlers[.]us (Source: [urlscan](https://urlscan.io))

The History tab in Hunt features a time graph that helps identify overlaps in port and certificate activity. Each button is clickable and displays additional information, such as **JA4X**, **JARM hashes**, and **certificate details**.

As shown in Figure 3, the cert's common name matches that of the malicious domain reported in the Rapid7 report, which is still active. Additionally, a JARM hash (the yellow bar at the bottom) will be helpful when crafting our detection query.

## 64.95.10.243 - Overview

Info Domains 1 History (Beta) Associations 2 SSL History SSH History JARM Port History Signals Activity 0

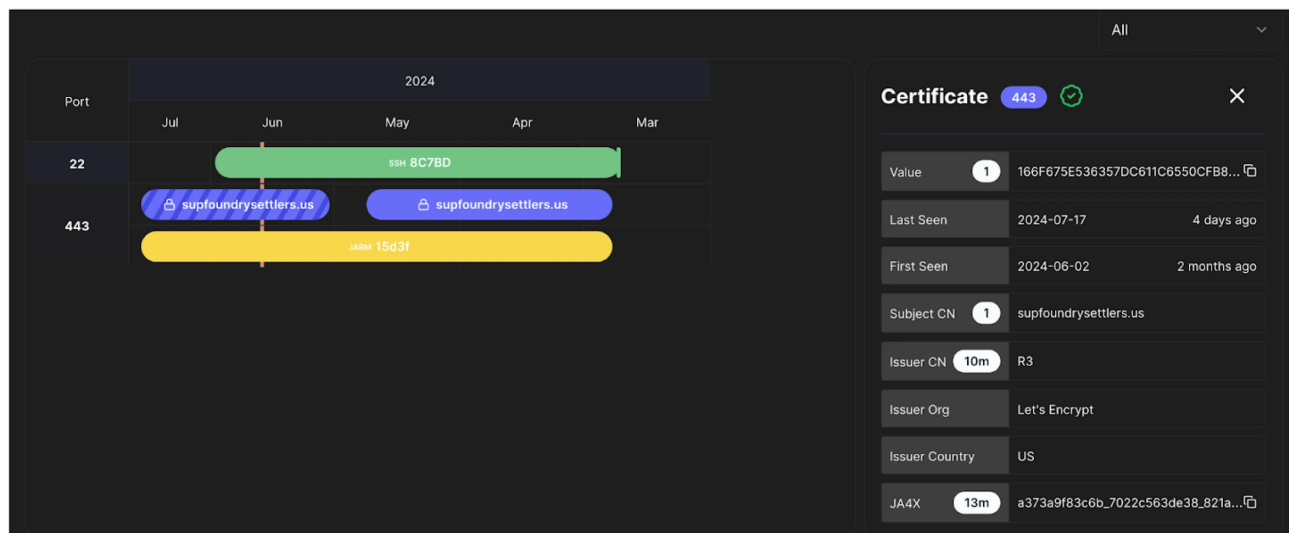


Figure 3: Screenshot of certificate information using the History tab

With no available pivots on port 22, SSH, or other TLS history, it's time to focus on developing a method for identifying the backdoor. Using Let's Encrypt certificates is common practice and would likely result in hundreds of thousands of results alone, but how many web pages have the title 'Soon'?

To understand the prevalence, we'll combine the cert's JARM fingerprint hash with the HTML response body hash. This approach may yield fewer results than searching for specific TLDs using Let's Encrypt.

With that, a pseudocode query to find additional Oyster servers is

```
jarm_fingerprint:"15d3fd16d29d29d00042d43d00000ed1cf37c9a169b41886e27ba8fad60b0"  
AND http_response_hash:"0c90ad9910cfb37c9969e14388707ef765ef5e73"
```

## Our Findings

Our detection rule for locating Oyster infrastructure flagged seven IP addresses, including the three mentioned in the Rapid7 post.

The limited number of results, combined with the already confirmed domain indicators, suggests our query is effective and likely on target until the threat actor decides to change up their C2 TTPs.

Let's Encrypt certificates and ports remained consistent across the returned results, with one exception (193.43.104[.]208), which had ports 80 and 443 open.

A notable difference is the ASNs. The three known domains/IPs were hosted on BL Networks infrastructure, while our findings are hosted on OVH SAS.

Below are the domains we have uncovered, which have a similar naming theme to those mentioned above.

\*Detailed information, including the corresponding IP addresses, can be found at the end of this article.

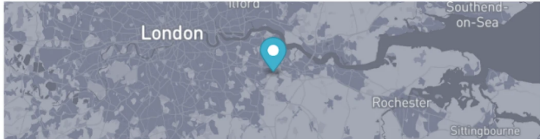
## - codeforprofessionalusers[.]com

### 51.195.232.46 - Overview

Info Domains 1 History (Beta) Associations 0 SSL History SSH History JARM Port History Signals Activity 0

51.195.232.46

OVH Ltd



Bexley, England, GB

**DNS**

Reverse DNS undefined

Forward DNS codeforprofessionalusers.com... 1

Tag

**ASN**

AS16276	51.195.0/16	OVH SAS
---------	-------------	---------

**Open Ports and Software**

Name	Port	Product	Version	Extra Info	Last Seen	First Seen	
SSH	22	-	-	-	1 week ago	10 months ago	🔍
TLS/HTTP	443	HTTPD	2.4.52	-	3 days ago	3 weeks ago	🔍

Figure 4: Overview of suspected Oyster backdoor IP (Check it out [here](#))

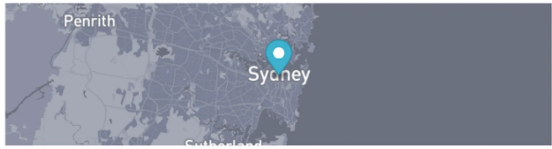
## - postmastersoriginals[.]com

# 139.99.221.140 - Overview

Info Domains 1 History (Beta) Associations 0 SSL History SSH History JARM Port History Signals Activity 1

139.99.221.140

OVH Australia PTY LTD



Sydney, New South Wales, AU

### DNS

Reverse DNS: undefined

Forward DNS: postmastersoriginals.com... 1

Tag

### ASN

AS16276 139.99.128.0/17 OVH SAS

### Open Ports and Software

Name	Port	Product	Version	Extra Info	Last Seen	First Seen
SSH	22	-	-	-	1 week ago	1 year ago
TLS/HTTP	443	HTTPD	2.4.52	-	2 weeks ago	8 months ago

Figure 5: Screenshot showing suspicious domain and ports 22, 443 (Check it out [here](#)) - firstcountryours[.]eu

# 162.19.237.181 - Overview

Info Domains 1 History (Beta) Associations 0 SSL History SSH History JARM Port History Signals Activity 0

162.19.237.181

OVH GmbH

Frankfurt am Main, Hesse, DE

### DNS

Reverse DNS undefined

Forward DNS firstcountryours.eu... **1**

Tag

### ASN

AS16276	162.19.128.0/17	OVH SAS
---------	-----------------	---------

### Open Ports and Software

Name	Port	Product	Version	Extra Info	Last Seen	First Seen	
SSH	22	-	-	-	2 weeks ago	1 year ago	
HTTP	443	HTTPD	2.4.52	-	1 day ago	1 year ago	

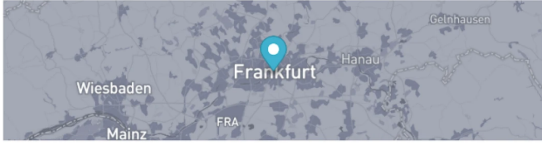
Figure 6: Overview of 162.19.237[.]181 and firstcountryours[.]eu (Check it out [here](#)) - dotnetisforchildren[.]com

## 193.43.104.208 - Overview

Info Domains 1 History (Beta) Associations 0 SSL History SSH History JARM Port History Signals Activity 0

193.43.104.208

BlueVPS OU



Frankfurt am Main, Hesse, DE

DNS

Reverse DNS mwka96bj128g6.easyinsurancequotes.net

Forward DNS dotnetisnotforchildren.com... 1

Tag

ASN

AS16276 193.43.104.0/24 OVH SAS

Open Ports and Software

Name	Port	Product	Version	Extra Info	Last Seen First Seen	
HTTP	80	HTTPD	2.4.52	-	2 days ago 1 year ago	🔍
TLS/HTTP	443	HTTPD	2.4.52	-	2 days ago 1 year ago	🔍

Figure 7: Screenshot of 193.43.104[.]208. Note ports 80 & 443 (link [here](#))

To further corroborate our findings associated with the Oyster backdoor, we can analyze the domains using VirusTotal.

It's important to note that a **VirusTotal score of 0 does not necessarily indicate that an IP or domain is benign**; it simply suggests that additional data may be required for a definitive assessment.

Below are the results for codeforprofessionalusers[.]com and postmastersoriginals[.]com.

Notably, CleanUp.dll has been linked to the Oyster backdoor. Furthermore, additional files appear to spoof Microsoft's Defender, potentially indicating a campaign aimed at users seeking antivirus software.

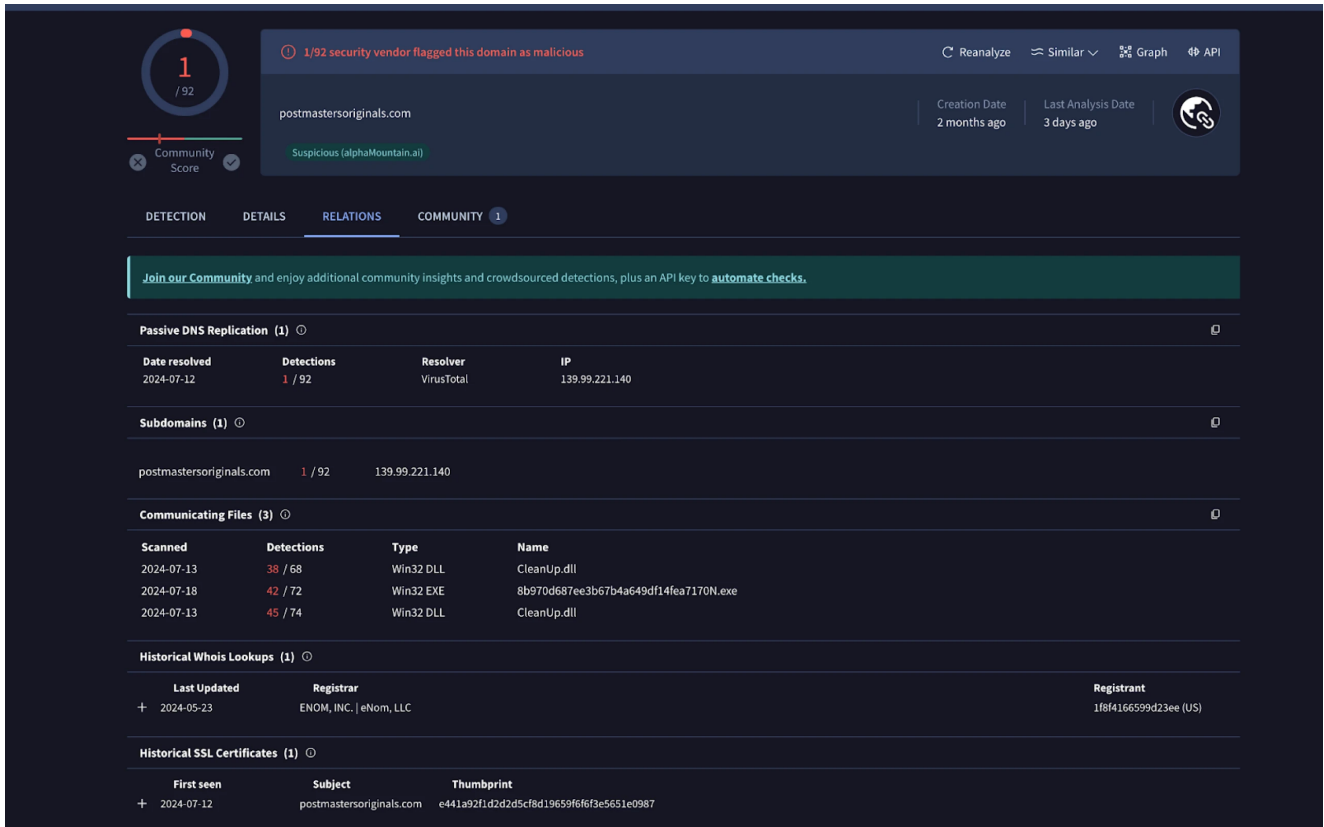


Figure 8: VirusTotal results for postmastersonline.com (Source: [VT](#))

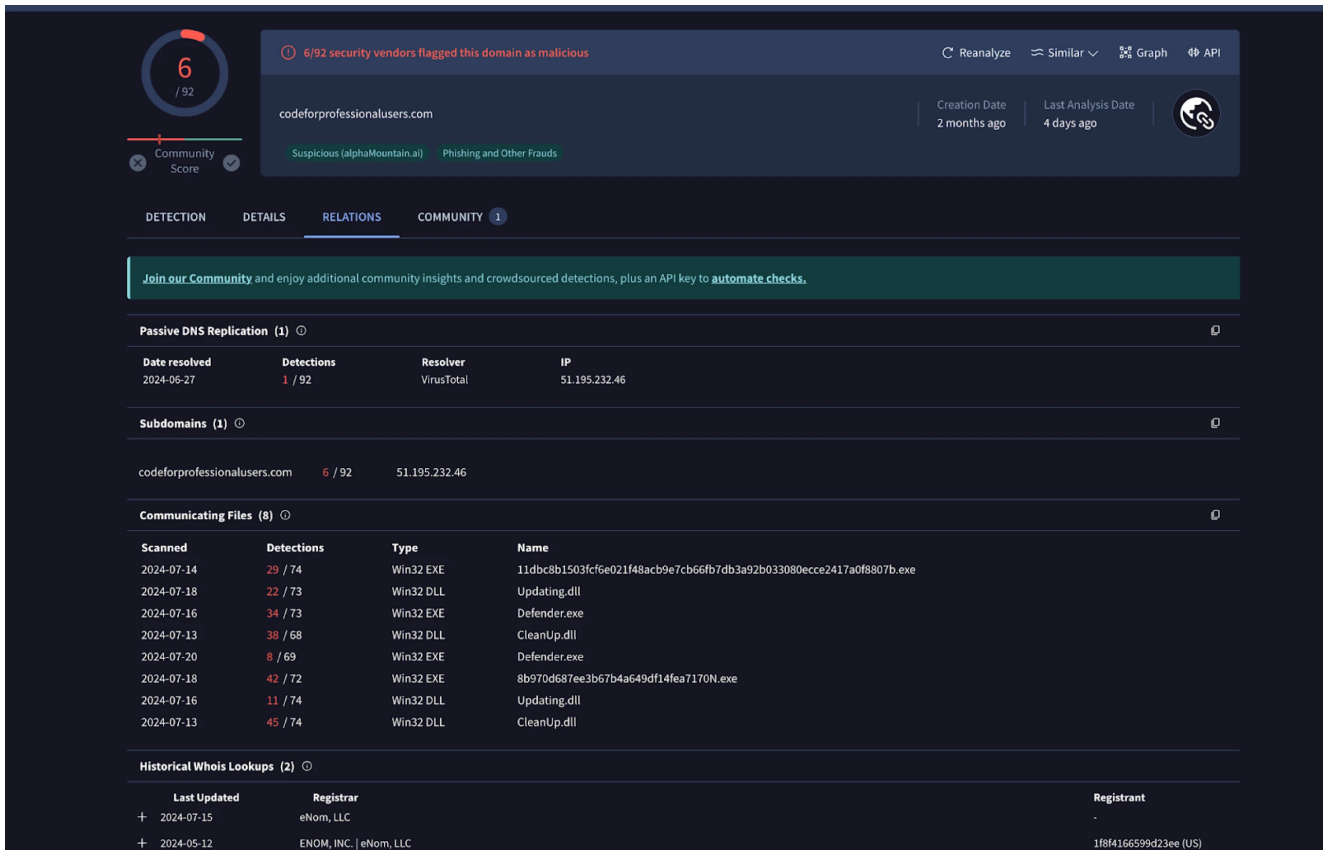


Figure 9: Screenshot of VT results for codeforprofessionalusers.com (Source: [VirusTotal](#))



Digging into any one of the CleanUp.dll files in Figure 10 below reveals a positive detection for the Oyster backdoor and the `/api/connectivity` URL path where victim information is sent via a POST request.

Additionally, under 'Contacted Domains,' we see one of our other finds, `firstcountryours[.]eu` listed.

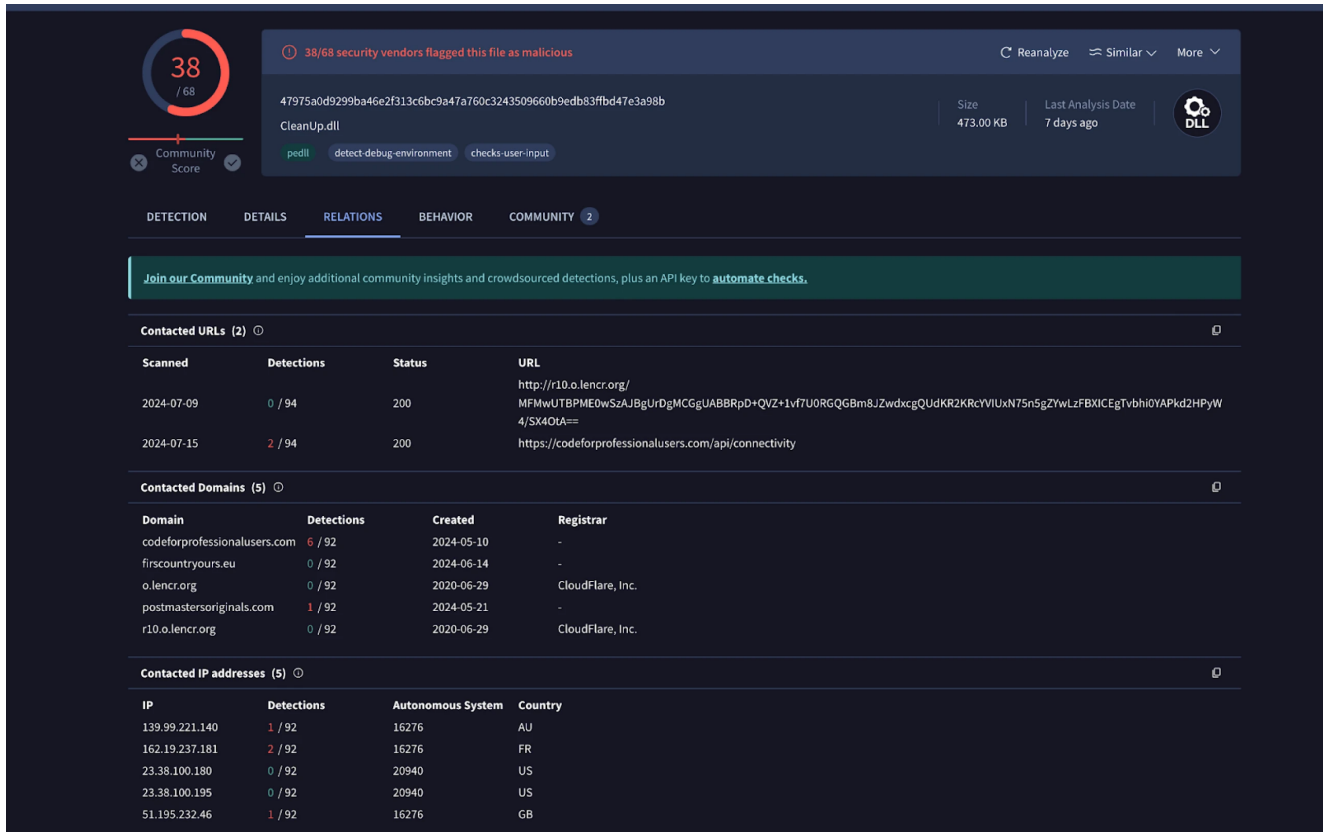


Figure 10: VirusTotal results for contacted URLs and domains of CleanUp.dll (Source: [VT](#))

## Conclusion

We uncovered and validated suspected Oyster backdoor infrastructure with a relatively simple query. While identifying malicious infrastructure can sometimes be straightforward, it's not always this easy and requires thorough analysis and strategic pivots to uncover additional C2s.

If you'd like to see how Hunt can help you expose malicious infrastructure before it's weaponized, contact us to [book a free demo](#) today.

## Network Observables

IP Address	Domain	ANS	Notes
64.95.10[.]243	supfoundrysettlers[.]us	BL Networks	Rapid7 Blog

<b>IP Address</b>	<b>Domain</b>	<b>ANS</b>	<b>Notes</b>
149.248.79[.]62	wherehomebe[.]com	BL Networks	Rapid7 Blog
206.166.251[.]114	retdirectyourman[.]eu	BL Networks	Rapid7 Blog
51.195.232[.]46	codeforprofessionalusers[.]com	OVH SAS	Jarm fingerprint + HTML response hash
139.99.221[.]140	postmastersoriginals[.]com	OVH SAS	Jarm fingerprint + HTML response hash
162.19.237[.]181	firstcountryours[.]eu	OVH SAS	Jarm fingerprint + HTML response hash
193.43.104[.]208	dotnetisforchildren[.]com	OVH SAS	Jarm fingerprint + HTML response hash