# A Simple Approach to Discovering Oyster Backdoor Infrastructure

Status hunt.io/blog/a-simple-approach-to-discovering-oyster-backdoor-infrastructure

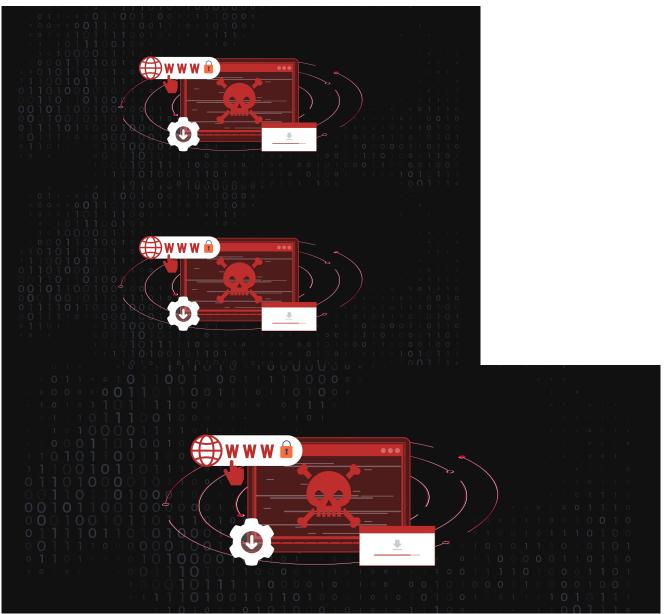


TABLE OF CONTENTS

## Introduction

Oyster backdoor, also known as Broomstick (<u>IBM</u>) and CleanUpLoader (<u>RussianPanda – X</u>), has been linked to malvertising campaigns mimicking popular software. On June 21st, <u>Rapid7</u> 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=eyJpdil6ImxkakluU1JRWVhwNkcrTlVEcFNndEE9PSIsInZhbHVlIjoid1RqRTlj
Set-Cookie: laravel_session=eyJpdiI6IllkdzdCeEhiWHA3a1ZvOGFENU01cWc9PSIsInZhbHVlIjoiUXc
Vary: Accept-Encoding
Content-Encoding: gzip Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
content-Type: text/ntmi; charset-off-6
html
<html lang="en"></html>
<head></head>
<meta charset="utf-8"/>
<pre><meta content="width=device-width, initial-scale=1" name="viewport"/></pre>
<title>Soon</title>
<body class="font-sans antialiased dark:bg-black dark:text-white/50"></body>
Soon
matches : [ »
0 : { »
description : Apache
parameters : { »
service.vendor : Apache
service.product : HTTPD
service.family : Apache
service.version : 2.4.52
<pre>service.cpe23 : cpe:/a:apache:http_server:{service.version}</pre>
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.

×

urlscan.ic	Alloma O Saara		Does 🜈 Drising 🕛 Login	SecurityTrails lecorded Future' Company
supfound				o To C Rescan
64.95.10.243				rdict
Submitted URL: ht				
Effective URL: http Submission: On July 2				
<b>∱</b> Summary ₩				
Summary				thot 🕽 🕈 Full Image
This website cor				
The main IP is 6				
main domain is s				
TLS certificate: I				
supfoundrysettle				
urlscan.io Ve				
Live informa				
Google Safe Bro				
Current DNS A				
Domain & IP ir				
IP/ASNs IP				Show full URLs
	IP Address	AS Autonomous System	1. http://supfoundrysettlers.us/ HTTP 307	
2	64.95.10.243 💻	399629 (BLNWX)	https://supfoundrysettlers.us/ Page URL	
2	1		Detected technologies	
			See Laravel (Web Frameworks)	Expand
			Page Statistics	
			2 100 % 0 %	1 1

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

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.

Info	Domains	Hist	cory (Beta)	Associations 2	SSL History	SSH History	JARM	Port History	Signals Activity	0	
										All	~
	Port			2024					Certificate	443	×
		Jul	Jun	Мау	Apr	Mar					
	22			ssн 8C7BD					Value 1	166F675E536357DC	611C6550CFB8 🗅
	443	🛆 supfour	ndrysettlers.us		oundrysettlers.us				Last Seen	2024-07-17	4 days ago
				JARM 15d3f					First Seen	2024-06-02	2 months ago
									Subject CN 1	supfoundrysettlers.u	s
									Issuer CN 10m	R3	
									Issuer Org	Let's Encrypt	
									Issuer Country	US	
									JA4X 13m	a373a9f83c6b_7022	c563de38_821af

#### 64.95.10.243 - Overview

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:"15d3fd16d29d29d00042d43d000000ed1cf37c9a169b41886e27ba8fad60b0" 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

AS16276     51.195.0.0/16     OVH SAS       pen Ports and Software         Name     Port     Product     Version       Extra Info     First Seen	L.195.232.46				DNS		
Forward DNS codeforprofessionalusers.com     Tag     ASN   AS16276   51.195.0.0/16      OVH SAS     SSH 2     1     Forward DNS   codeforprofessionalusers.com     Tag     ASN   AS16276   51.195.0.0/16   OVH SAS     SSH   1     Tag     Tag     Tag     Tag     SSH   1     Tag     Tag     Tag     SSH   1     Tag     Tag	OVH Ltd				Reverse DNS	undefined	
London   Rochester   xkey, England, GB •     ASN   AS16276   51.195.0.016   OVH SAS   per Ports and Software   Name   Port   Product   Version   Extra Info   First Seen   SSH   22     -     I week ago	y Ni teoryo	ittora			Forward DNS	codeforprofessionalusers.com.	. 1
Sittenapour       ASN         Asic276       51.195.0.0/16       OVH SAS         pen Ports and Software       Image: State Software       Image: State Software         Name       Port       Product       Version       Extra Info       Image: Software         SSH       22       -       -       1 week ago       Q	land in the	London			Tag		
Name     Port     Product     Version     Extra Info     First Seen       SSH     22     -     -     1 week ago     Q	exley England G		Rochester	Sittingbourne	ASN		
Name     Port     Product     Version     Extra Info     First Seen       SSH     22     -     -     1 week ago     Q	and, England, E				AS16276	51.195.0.0/16	OVH SAS
					AS16276	51.195.0.0/16	OVH SAS
	pen Ports and	l Software	Product	Version		Last Seen	OVH SAS

Figure 4: Overview of suspected Oyster backdoor IP (Check it out <u>here</u>) - postmastersoriginals[.]com

#### 139.99.221.140 - Overview

443

TLS/HTTP

HTTPD

39.99.221.14	40 🗖			DNS		
OVH Au	istralia PTY LTD			Reverse DNS	undefined	
			_	Forward DNS	postmastersoriginals.com	1
Penrith	Syune	ey		Tag		
12 F						
dney, New Sout	th Wales, AU 🛇			ASN		
/dney, New Sout	th Wales, AU 🛇			AS16276	139.99.128.0/17	OVH SAS
ydney, New Sout					139.99.128.0/17	OVH SAS

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

2.4.52

2 weeks ago

8 months ago

Q

#### 162.19.237.181 - Overview

2.19.237.181	DNS
) OVH GmbH	Reverse DNS undefined
OVH GmbH	Forward DNS firscountryours.eu 1
Gdithausen Frankfurt Wiesbaden	Tag
Mainz FRA	ASN
	AS16276 162.19.128.0/17 OVH SAS

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

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

93.43.104.208	8 🗇			DNS		
BlueVPS	OU		Reverse DNS mwka96bj128g6.easyinsurancequotes.net			
M See		Gelnhausen	*	Forward DNS do	tnetisnotforchildren.com	
And the second	Frankfur	t Hanau	Jose Hora	Tag		
Wiesbade	FRA.		or			
rankfurt am Main,	Hesse, DE 🛇			ASN		
				AS16276 1	93.43.104.0/24	OVH SAS
				AS16276 1	93.43.104.0/24	OVH SAS
open Ports and	l Software			AS16276 1	93.43.104.0/24	OVH SAS
<b>Open Ports and</b> Name	<b>I Software</b> Port	Product	Version	AS16276 1 Extra Info	93.43.104.0/24 Last Seen First Seen	OVH SAS
Open Ports and Name HTTP		Product HTTPD	Version 2.4.52		Last Seen	OVH SAS

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.

								C Reanalyze	⇔ Similar ∨	💥 Graph	¢⊅ API
	(1)/92										
		postmastersorigin	als.com					Creation Date 2 months ago	Last Analysis 3 days ago		er de la comercia de
	Community Score										
	DETECTION D	ETAILS RELATION	IS COMMUNITY								
	Join our Community	rand oniou additional co	mmunituincighte and	crowdcourcod datact	ions, plus an API key to <u>aut</u> e	emate checks					
	John Car Community	and enjoy additional to	initiality insights and	crowdsourced detect	ions, plus an Ar i key to <u>aut</u>	onate checka.					
	Passive DNS Replicat	tion (1) ①									
	Date resolved 2024-07-12	Detections 1 / 92	<b>Resolver</b> VirusTotal	IP 139.99.	.221.140						
	Subdomains (1)										Q
	Subdomains (1) ①										U U
	postmastersoriginals.	com 1 / 92	139.99.221.140								
	Communicating Files	s (3) ①									
	Scanned	Detections	Туре	Name							
	2024-07-13	38 / 68	Win32 DLL	CleanUp.dll							
	2024-07-18	<mark>42</mark> / 72	Win32 EXE	8b970d687ee3	b67b4a649df14fea7170N.ex	e					
	2024-07-13	45 / 74	Win32 DLL	CleanUp.dll							
	Historical Whois Lool	kuns (1) ①									
		(a) (									
	Last Updated	Registrar							Re	gistrant	
			iom, LLC							<b>gistrant</b> 8f4166599d23e	e (US)
	Last Updated	<b>Registrar</b> ENOM, INC.   eN	lom, LLC								re (US)
	Last Updated + 2024-05-23 Historical SSL Certifi First seen	Registrar ENOM, INC.   eN cates (1) Subject	Thumb		2466140007						re (US)
	Last Updated + 2024-05-23 Historical SSL Certifit First seen + 2024-07-12	Registrar ENOM, INC.   eN cates (1) Subject postmastersorij	Thumb ginals.com e441a92f1	d2d2d5cf8d19659f6f6f							e (US)
Figure 8:	Last Updated + 2024-05-23 Historical SSL Certifit First seen + 2024-07-12	Registrar ENOM, INC.   eN cates (1) Subject postmastersorij	Thumb ginals.com e441a92f1	d2d2d5cf8d19659f6f6f	38555160987 Soriginals[.	]com (S	Source:	<u>VT</u> )			ње (US)
Figure 8:	Last Updated + 2024-05-23 Historical SSL Certifit First seen + 2024-07-12	Registrar ENOM, INC.   eN cates (1) © Subject postmastersorij	Thumb ginals.com e441a92f1 6 for post	dzdzd5cf8d19659f6f6f		]com (S	ource:	<u>VT</u> )			e (US)
Figure 8:	Last Updated + 2024-05-23 Historical SSL Certifit First seen + 2024-07-12	Registrar ENOM, INC.   eN cates (1) © Subject postmastersorij	Thumb ginals.com e441a92f1	dzdzd5cf8d19659f6f6f		]com (S	Source:	VT) C Reanalyze			
Figure 8:	Last Updated + 2024-05-23 Historical SSL Certifit First seen + 2024-07-12 : Virus Tot	Registrar ENOM, INC.   eN cates (1) © Subject postmastersori al results	Thumb ginals.com e441a92f1 6 for post vendors flagged this d	dzdzd5cf8d19659f6f6f		]com (S	Source:	<b>C</b> Reanalyze	1fe	14166599d23e	¢∳ API
Figure 8:	Last Updated + 2024-05-23 Historical SSL Certifit First seen + 2024-07-12 : Virus Tot	Registrar ENOM, INC.   eN cates (1) © Subject postmastersorij	Thumb ginals.com e441a92f1 6 for post vendors flagged this d	dzdzd5cf8d19659f6f6f		]com (S	Source:	C Reanalyze	1fe ≈ Similar ∨	14166599d23e	
Figure 8:	Last Updated + 2024-05-23 Historical SSL Certifit First seen + 2024-07-12 : Virus Tot	Registrar ENOM, INC.   eN cates (1) © Subject postmastersorif al results © 6/92 security codeforprofession	Thumb ginals.com e441a92f1 6 for post vendors flagged this d	d2d2d5cf8d19659f6f6f masters		]com (S	Source:	<b>C</b> Reanalyze	1fe	14166599d23e	¢∳ API
Figure 8:	Last Updated + 2024-05-23 Historical SSL Certifit First seen + 2024-07-12 : Virus Tot 6 /92 & Community Score	Registrar ENOM, INC. J eN subject postmastersori al results 0 6/92 security codeforprofession Suspicious (alphak	thumb ginals.com e441a92f1 for post vendors flagged this d alusers.com Mountain.ai) Phishing a	d2d2dscf8d19659f6f6f masters Iomain as malicious nd Other Frauds		]com (S	ource:	<b>C</b> Reanalyze	1fe	14166599d23e	¢∳ API
Figure 8	Last Updated + 2024-05-23 Historical SSL Certifit First seen + 2024-07-12 : Virus Tot 6 /92 & Community Score	Registrar ENOM, INC.   eN cates (1) © Subject postmastersorif al results © 6/92 security codeforprofession	thumb ginals.com e441a92f1 for post vendors flagged this d alusers.com Mountain.ai) Phishing a	d2d2dscf8d19659f6f6f masters Iomain as malicious nd Other Frauds		]com (S	Source:	<b>C</b> Reanalyze	1fe	14166599d23e	¢∳ API
Figure 8	Last Updated + 2024-05-23 Historical SSL Certifit First seen + 2024-07-12 : Virus Tot 6 /92 © Community Score DETECTION D	Registrar ENOM, INC. J eN subject postmastersorif al results of 6/92 security codeforprofession Suspicious (alphak	Thumb ginals.com e441a92f1 6 for post vendors flagged this d alusers.com Aountain.ai) Phishing a is COMMUNITY	dzdzascted19659fefef masters Iomain as malicious Ind Other Frauds	soriginals[.		Source:	<b>C</b> Reanalyze	1fe	14166599d23e	¢∳ API
Figure 8	Last Updated + 2024-05-23 Historical SSL Certifit First seen + 2024-07-12 : Virus Tot 6 /92 © Community Score DETECTION D	Registrar ENOM, INC. J eN subject postmastersorif al results of 6/92 security codeforprofession Suspicious (alphak	Thumb ginals.com e441a92f1 6 for post vendors flagged this d alusers.com Aountain.ai) Phishing a is COMMUNITY	dzdzascted19659fefef masters Iomain as malicious Ind Other Frauds			Source:	<b>C</b> Reanalyze	1fe	14166599d23e	¢∳ API
Figure 8	Last Updated + 2024-05-23 Historical SSL Certifit First seen + 2024-07-12 : Virus Tot 6 /92 © Community Score DETECTION D	Registrar ENOM, INC. J eN subject postmastersorij al results () 6/92 security codeforprofession Suspicious (alphak ETAILS RELATION	Thumb ginals.com e441a92f1 6 for post vendors flagged this d alusers.com Aountain.ai) Phishing a is COMMUNITY	dzdzascted19659fefef masters Iomain as malicious Ind Other Frauds	soriginals[.		Source:	<b>C</b> Reanalyze	1fe	14166599d23e	¢∳ API

Community		onalusers.com naMountain.ai) Phishing ai	id Other Frauds	2 months ago 4 d	days ago	C.9
Score	Suspicious (aiph	amountain.ai) Phisning a	d Other Frauds			
DETECTION	DETAILS RELATIO	DNS COMMUNITY				
<u>Join our Commu</u>	<u>nity</u> and enjoy additional	community insights and o	rowdsourced detections, plus an API key to automate checks.			
Passive DNS Repl	ication (1) ①					c
Date resolved 2024-06-27	Detections 1 / 92	<b>Resolver</b> VirusTotal	IP 51.195.232.46			
						C
Subdomains (1)						
Subdomains (1) codeforprofession Communicating F	alusers.com 6 / 92	51.195.232.46				
codeforprofession	alusers.com 6 / 92	51.195.232.46 <b>Type</b>	Name			
codeforprofession Communicating F	alusers.com 6 / 92		Name 11dbc8b1503fcf6e021f48acb9e7cb66fb7db3a92b033080ecce2417a0f8807b.ex	œ		
codeforprofession Communicating F Scanned	alusers.com 6 / 92 Files (8) ① Detections	Туре		ĸe		
codeforprofession Communicating F Scanned 2024-07-14	alusers.com 6 / 92 Files (8) © Detections 29 / 74	Type Win32 EXE	11dbc8b1503fcf6e021f48acb9e7cb66fb7db3a92b033080ecce2417a0f8807b.ex	xe		
codeforprofession Communicating F Scanned 2024-07-14 2024-07-18	alusers.com 6 / 92 Files (8) © Detections 29 / 74 22 / 73	<b>Type</b> Win32 EXE Win32 DLL	11dbc8b1503fcf6e021f48acb9e7cb66fb7db3a92b033080ecce2417a0f8807b.ex Updating.dll	ĸe		
codeforprofession Communicating F Scanned 2024-07-14 2024-07-18 2024-07-16	alusers.com 6 / 92 Files (8) © Detections 29 / 74 22 / 73 34 / 73	<b>Type</b> Win32 EXE Win32 DLL Win32 EXE	11dbc8b1503fcf6e021f48acb9e7cb66fb7db3a92b033080ecce2417a0f8807b.ex Updating.dll Defender.exe	æ		
codeforprofession Communicating F Scanned 2024-07-14 2024-07-18 2024-07-16 2024-07-13	alusers.com 6 / 92 Files (8) © Detections 29 / 74 22 / 73 34 / 73 38 / 68	<b>Type</b> Win32 EXE Win32 DLL Win32 EXE Win32 DLL	11dbc8b1503fcf6e021f48acb9e7cb66fb7db3a92b033080ecce2417a0f8807b.ex Updating.dll Defender.exe CleanUp.dll	œ		
codeforprofession Communicating F Scanned 2024-07-14 2024-07-18 2024-07-16 2024-07-13 2024-07-20	alusers.com 6 / 92 files (8) © Detections 29 / 74 22 / 73 34 / 73 38 / 68 8 / 69	Type Win32 EXE Win32 DLL Win32 EXE Win32 DLL Win32 EXE	11dbc8b1503fcf6e021f48acb9e7cb66fb7db3a92b033080ecce2417a0f8807b.ex Updating.dll Defender.exe CleanUp.dll Defender.exe	œ		
codeforprofession Communicating F Scanned 2024-07-14 2024-07-18 2024-07-16 2024-07-13 2024-07-20 2024-07-20	alusers.com 6 / 92 files (8) © Detections 29 / 74 22 / 73 34 / 73 38 / 68 8 / 69 42 / 72	Type Win32 EXE Win32 DLL Win32 EXE Win32 EXE Win32 EXE Win32 EXE	11dbc8b1503fcf6e021f48acb9e7cb66fb7db3a92b033080ecce2417a0f8807b.ex Updating.dll Defender.exe CleanUp.dll Defender.exe 8b970d687ee3b67b4a649df14fea7170N.exe	œ		
codeforprofession Communicating F Scanned 2024-07-14 2024-07-18 2024-07-18 2024-07-18 2024-07-13 2024-07-18 2024-07-18 2024-07-18	alusers.com 6 / 92 Files (8) © Detections 29 / 74 22 / 73 34 / 73 38 / 68 8 / 69 42 / 72 11 / 74 45 / 74	Type Win32 EXE Win32 DLL Win32 EXE Win32 EXE Win32 EXE Win32 EXE Win32 DLL	11dbc8b1503fcf6e021f48acb9e7cb66fb7db3a92b033080ecce2417a0f8807b.ex Updating.dll Defender.exe CleanUp.dll Defender.exe 8b970d687ee3b67b4a649df14fea7170N.exe Updating.dll	/e		0

 +
 2024/05-12
 ENOM, INC. [ eNOM, ILC
 108/16/05/99/23/24 (US)

 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.

				${ m C}$ Reanalyze $symp $ Similar $$ More $$
38				
(68) Community Score	CleanUp.dll	e2f313c6bc9a47a760c324	3509660b9edb83ffbd47e3a98b ser-input	Size Last Analysis Date A73.00 KB 7 days ago
Score				
DETECTION D	DETAILS RELATIONS	BEHAVIOR	COMMUNITY 2	
Join our Community	y and enjoy additional cor	nmunity insights and crow	dsourced detections, plus an API key to <b>automate checks.</b>	
Contacted URLs (2)				
Scanned	Detections	Status	URL	
			http://r10.o.lencr.org/	
2024-07-09	0 / 94	200	MFMwUTBPME0wSzAJBgUrDgMCGgUABBRpD+QVZ+1vf7U0RGQGBm8JZv 4/SX4OtA==	wdxcgQUdKR2KRcYVIUxN75n5gZYwLzFBXICEgTvbhi0YAPkd2HPyW
2024-07-15	2 / 94	200	https://codeforprofessionalusers.com/api/connectivity	
Contacted Domains				
Contacted Domains Domain		Created	Registrar	0
	(5) ① Detections			0 0
Domain	(5) ① Detections	Created		o
Domain codeforprofessionalu	(5) ① Detections Isers.com 6 / 92	<b>Created</b> 2024-05-10	Registrar	0
Domain codeforprofessionalu firscountryours.eu	(5) ① seers.com 6 / 92 0 / 92 0 / 92	Created 2024-05-10 2024-06-14	Registrar -	0
Domain codeforprofessionalu firscountryours.eu o.lencr.org	(5) ① seers.com 6 / 92 0 / 92 0 / 92	Created 2024-05-10 2024-06-14 2020-06-29	Registrar -	o
Domain codeforprofessionalu firscountryours.eu o.lencr.org postmastersoriginals	(5) beta beta beta beta beta beta beta beta	Created 2024-05-10 2024-06-14 2020-06-29 2024-05-21	Registrar - - CloudFlare, Inc. -	0
Domain codeforprofessionalu firscountryours.eu o.lencr.org postmastersoriginals r10.o.lencr.org	(5) beta beta beta beta beta beta beta beta	Created 2024-05-10 2024-06-14 2020-06-29 2024-05-21	Registrar - - CloudFlare, Inc. - CloudFlare, Inc.	
Domain codeforprofessionalu firscountryours.eu o.lencr.org postmastersoriginals r10.o.lencr.org Contacted IP address	(5) © sers.com 6 / 92 0 / 92 0 / 92 0 / 92 0 / 92 0 / 92 9 / 92 9 / 92 0 / 92	<b>Created</b> 2024-05-10 2024-06-14 2020-06-29 2024-05-21 2020-06-29	Registrar - - CloudFlare, Inc. - CloudFlare, Inc.	
Domain codeforprofessionalu firscountryours.eu o.lencr.org postmastersoriginals r10.o.lencr.org Contacted IP address IP	(5) © sees.com 6 / 92 0 / 92 0 / 92 1 / 92 0 / 92 9 / 92 sees (5) © Detections	Created 2024-05-10 2024-06-14 2020-06-29 2024-05-21 2020-06-29 Autonomous System	Registrar - - CloudFlare, Inc. - CloudFlare, Inc.	
Domain codeforprofessionalu firscountryours.eu o.lencr.org postmastersoriginals r10.o.lencr.org Contacted IP address IP 139.99.221.140	(5) ○ sers.com 6/92 0/92 0/92 1/92 0/92 0/92 1/92 betections 1/92	Created 2024-05-10 2024-06-14 2020-06-29 2024-05-21 2020-06-29 2020-06-29	Registrar - - CloudFlare, Inc. - CloudFlare, Inc. - CloudFlare, Inc.	
Domain codeforprofessionalu firscountryours.eu o.lencr.org postmastersoriginals r10.o.lencr.org Contacted IP address IP 139.99.221.140 162.19.237.181	(5) ○ sers.com 6/92 0/92 0/92 1/92 0/92 1/92 ses (5) ○ Detections 1/92 2/92	Created 2024-05-10 2024-06-14 2020-06-29 2024-05-21 2020-06-29 2020-06-20 200-06-20 200-06-20 200-06-20 200-06-20 200-06-20 200-06-20 200-06-20 200-06-20 200-06-20 200-06-20 200-06-20 200-06-20 200-06-20 200-06-20 200-06-20 200-06-20 200-06-20 200-06-20	Registrar - - CloudFlare, Inc. - CloudFlare, Inc. Country AU FR	

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 <u>book a free demo</u> 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.



Figure 1: Underlined HTML title for 64.95.10[.]243 (Try it <u>here</u>) An additional screenshot of the above webpage from urlscanio can be found below. ×

urlscan.ic	Alloma O Saara		Does 🜈 Drising 🕛 Login	SecurityTrails lecorded Future' Company
supfound				o To C Rescan
64.95.10.243				rdict
Submitted URL: ht				
Effective URL: http Submission: On July 2				
<b>∱</b> Summary ₩				
Summary				thot 🕽 🕈 Full Image
This website cor				
The main IP is 6				
main domain is s				
TLS certificate: I				
supfoundrysettle				
urlscan.io Ve				
Live informa				
Google Safe Bro				
Current DNS A				
Domain & IP ir				
IP/ASNs IP				Show full URLs
	IP Address	AS Autonomous System	1. http://supfoundrysettlers.us/ HTTP 307	
2	64.95.10.243 💻	399629 (BLNWX)	https://supfoundrysettlers.us/ Page URL	
2	1		Detected technologies	
			See Laravel (Web Frameworks)	Expand
			Page Statistics	
			2 100 % 0 %	1 1

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

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.

Info	Domains	1 Hist	ory (Beta)	Associations 2	SSL History	SSH History	JARM	Port History	Signals Activity	0	
										All	~
	Port			2024					Certificate	443 🕑	×
		Jul	Jun	May	Apr	Mar					
	22			SSH 8C7BD					Value 1	166F675E536357DC	:611C6550CFB8 🗅
	443	🛆 supfoun	drysettlers.us		oundrysettlers.us				Last Seen	2024-07-17	4 days ago
				JARM 15d3f					First Seen	2024-06-02	2 months ago
									Subject CN 1	supfoundrysettlers.u	IS
									Issuer CN 10m	R3	
									Issuer Org	Let's Encrypt	
									Issuer Country	US	
									JA4X 13m	a373a9f83c6b_7022	cc563de38_821aC

#### 64.95.10.243 - Overview

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:"15d3fd16d29d29d00042d43d000000ed1cf37c9a169b41886e27ba8fad60b0" 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

l.195.232.46				DNS		
OVH Ltd				Reverse DNS undefined		
	lliora		Southend-	Forward DNS	codeforprofessionalusers.com.	. 1
The State	London	NAL -		Tag		
		Rochester	Sittingbourne	ASN		
xley, England, GE	3 ©			A311		
xley, England, GE	3 ©			AS16276	51.195.0.0/16	OVH SAS
					51.195.0.0/16	OVH SAS
					51.195.0.0/16	OVH SAS
xley, England, GE Den Ports and Name		Product	Version		51.195.0.0/16 Last Seen First Seen	OVH SAS

Figure 4: Overview of suspected Oyster backdoor IP (Check it out <u>here</u>) - postmastersoriginals[.]com

#### 139.99.221.140 - Overview

TLS/HTTP

- firstcountryours[.]eu

443

HTTPD

39.99.221.14	40 🗉			DNS		
OVH Australia PTY LTD				Reverse DNS	undefined	
Penrith		M.		Forward DNS	postmastersoriginals.com	1
Pennth	Syune	ý		Tag		
A L						
dney, New Sou	Sutherland Ith Wales, AU 🛇			ASN		
rdney, New Sou	stelestere			ASN AS16276	139.99.128.0/17	OVH SAS
	nth Wales, AU S				139.99.128.0/17	OVH SAS

2.4.52

Figure 5: Screenshot showing suspicious domain and ports 22, 443 (Check it out here)

2 weeks ago

8 months ago

Q

#### 162.19.237.181 - Overview

2.19.237.181	DNS		
OVH GmbH	Reverse DNS	undefined	
etinharsan	Forward DNS	firscountryours.eu	
Wiesbaden	Tag		
Mainz FRA	ASN		
	AS16276	162.19.128.0/17	OVH SAS

and Software					
Port	Product	Version	Extra Info	Last Seen First Seen	
22	-	-	-	2 weeks ago 1 year ago	Q
443 57	HTTPD	2.4.52	-	1 day ago 1 year ago	Q
	22	Port Product	Port Product Version	Port Product Version Extra Info 22	Port     Product     Version     Extra Info     Last Seen First Seen       22     -     -     -     2 weeks ago 1 year ago       443 °     HTTPD     2.4.52     -     1 day ago

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

93.43.104.208				DNS Reverse DNS mwka96bj128g6.easyinsurancequotes.net		
BlueVPS	OU					
Wiesbade	n Frankfur	Gelnhausen Hanau	Forward DNS dotn Tag	etisnotforchildren.com 1	•	
Mainz	FRA		i.	ASN		
ankturt am Main,	Hesse, DE 🛇					
ankfurt am Main,	Hesse, DE 🛇			AS16276 19	3.43.104.0/24	OVH SAS
pen Ports and		Product	Version	AS16276 19 Extra Info	3.43.104.0/24 Last Seen First Seen	OVH SAS

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.

	① 1/92 security vendor flagged this domain as malicious	C Reanalyze $\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \$	쁆 Graph 💠 API
			s Date
	postmastersoriginals.com	2 months ago 3 days ago	s Date
	Community Score Suspicious (alphaMountain.ai)		
	DETECTION DETAILS RELATIONS COMMUNITY 1		
	Join our Community, and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.		
	Passive DNS Replication (1) O		
	Date resolved         Detections         Resolver         IP           2024-07-12         1 / 92         VirusTotal         139.99.221.140		
	Subdomains (1) O		
	postmastersoriginals.com 1 / 92 139.99.221.140		
	Communicating Files (3) O		
	Scanned Detections Type Name		
	2024-07-13 38 / 68 Win32 DLL CleanUp.dll 2024-07-18 42 / 72 Win32 EXE 8b970d687ee3b67b4a649df14fea7170N.exe		
	2024-07-18 42 / 72 Win32 EXE 8b970d687ee3b67b4a649df14fea7170N.exe 2024-07-13 45 / 74 Win32 DLL CleanUp.dll		
	Historical Whois Lookups (1) O		
	Historical Whois Lookups (1) © Last Updated Registrar + 2024-05-23 ENOM, INC.   eNom, LLC		gistrant if4166599d23ee (US)
	Last Updated Registrar		
	Last Updated Registrar + 2024-05-23 ENOM, INC.   eNom, LLC		
Figure 8:	Last Updated Registrar + 2024-05-23 ENOM, INC.   eNom, LLC Historical SSL Certificates (1) O First seen Subject Thumbprint	μ Ι	
Figure 8:	Last Updated     Registrar       +     2024-05-23     ENOM, INC.   eNom, LLC       Historical SSL Certificates     I)     O       -     First seen     Subject     Thumbprint       +     2024-07-12     postmastersoriginals.com     e441a92f1d2d2d5cf8d19659f6f6fB8e5651e0987	μ Ι	
Figure 8:	Last Updated     Registrar       +     2024-05-23     ENOM, INC.   eNom, LLC       Historical SSL Certificates     I)     O       -     First seen     Subject     Thumbprint       +     2024-07-12     postmastersoriginals.com     e441a92f1d2d2d5cf8d19659f6f6fB8e5651e0987	μ Ι	1/4166599d23ee (US)
Figure 8:	Last Updated     Registrar       + 2024-05-23     ENOM, INC. JeNom, LLC       Historical SSL Certificates (1) ©     Thumbprint       + 2024-07-12     postmastersoriginals.com       e441a92f1d2d2dscR8196559666f3265551e0987       VirusTotal results for postmastersoriginals[.]com (Source:       6 /92	۱۳ <u>VT</u> ) C Reanalyze	14166599d23ee (US)
Figure 8:	Last Updated     Registrar       + 2024-05-23     ENOM, INC. [eNom, LLC       Historical SSL Certificates (1) ©     •       First Seen     Subject     Thumbprint       + 2024-07-12     postmastersoriginals.com     •       Virus Total results for postmastersoriginals[.]com (Source:       6       72       6       72       6       72	⊥fr <u>VT</u> ) C Reanalyze ≈ Similar ~	14166599d23ee (US)
Figure 8:	Last Updated     Registrar       + 2024-05-23     ENOM, INC. JeNom, LLC       Historical SSL Certificates (1) ©     Thumbprint       + 2024-07-12     postmastersoriginals.com       e441a92f1d2d2dscR8196559666f3265551e0987       VirusTotal results for postmastersoriginals[.]com (Source:       6 /92	۱۳ <u>VT</u> ) C Reanalyze	14166599d23ee (US)
Figure 8:	Last Updated     Registrar       + 2024-05-23     ENOM, INC. [eNom, LLC       Historical SSL Certificates (1) ©     Immbprint       + 2024-07-12     postmastersoriginals.com       First seen     Subject       + 2024-07-12     postmastersoriginals.com       VirusTotal results for postmastersoriginals[.]com (Source:       6       /92       conformunity       6       /92       codeforprofessionalusers.com       Suspicious (alphaMountain.a)       Phishing and Other Fauds	۱۳ <u>VT</u> ) C Reanalyze	14166599d23ee (US)
Figure 8:	Last Updated     Registrar       + 2024-05-23     ENOM, INC. [eNom, LLC       Historical SSL Certificates (1) ©     Thumbprint       + 2024-07-12     postmastersoriginals.com       • 441.p92/Ld2d2d5c/8d19659/6/6/I2e5651e0987       Virus Total results for postmastersoriginals[.]com (Source:       • 6       • /92       • 6       • /92       • 6       • (9/92 security vendors flagged this domain as malicious       • codeforprofessionalusers.com       Score       • Suspicious (alphaMountain.al)       • Philshing and Other Frauds	۱۳ <u>VT</u> ) C Reanalyze	14166599d23ee (US)
Figure 8:	Last Updated       Registrar         +       2024-05-23       ENOM, INC. [eNom, LLC         Historical SSL Certificates (1) ©       •         +       2024-07-12       postmästersoriginals.com         •       Subject       Thumbprint         +       2024-07-12       postmästersoriginals.com         •       VirusTotal results for postmastersoriginals[.]com (Source:         •       6         •       •	۱۳ <u>VT</u> ) C Reanalyze	14166599d23ee (US)

	codeforprofessio	onalusers.com	Creation D 2 months		6
Community.					
Score Score	Suspicious (alph	aMountain.ai) Phishing a	nd Other Frauds		
DETECTION	DETAILS RELATIO	ONS COMMUNITY			
Join our Commun	ity and enjoy additional (	community insights and o	crowdsourced detections, plus an API key to automate checks.		
Passive DNS Replic	ation (1) ①				
Date resolved	Detections	Resolver	IP		
2024-06-27	1 / 92	VirusTotal	51.195.232.46		
Subdomains (1)	D				Q
Subdomains (1)					Q
Subdomains (1) (		51.195.232.46			O
codeforprofessiona	users.com 6 / 92	51.195.232.46			
	users.com 6 / 92	51.195.232.46			
codeforprofessiona	users.com 6 / 92	51.195.232.46 <b>Type</b>	Name		
codeforprofessiona Communicating Fi	lusers.com 6 / 92		Name 11dbc8b1503fcfGe021f48acb9e7cb66fb7db3a92b033080ecce2417a0f8807b.exe		
codeforprofessiona Communicating Fi Scanned	lusers.com 6 / 92 les (8) ① Detections	Туре			
codeforprofessiona Communicating Fi Scanned 2024-07-14	users.com 6 / 92 les (8) © Detections 29 / 74	Type Win32 EXE	11dbc8b1503fcf6e021f48acb9e7cb66fb7db3a92b033080ecce2417a0f8807b.exe		
codeforprofessiona Communicating Fi Scanned 2024-07-14 2024-07-18	Lusers.com 6 / 92 Les (8) © Detections 29 / 74 22 / 73	<b>Type</b> Win32 EXE Win32 DLL	11dbc8b1503fcf6e021f48acb9e7cb66fb7db3a92b033080ecce2417a0f6807b.exe Updating.dll		
codeforprofessiona Communicating Fi Scanned 2024-07-14 2024-07-18 2024-07-16	Lusers.com 6 / 92 les (8) © Detections 29 / 74 22 / 73 34 / 73	<b>Type</b> Win32 EXE Win32 DLL Win32 EXE	11dbc8b1503fcf6e021f48acb9e7cb66fb7db3a92b033080ecce2417a0f8807b.exe Updating.dll Defender.exe		
codeforprofessiona Communicating Fi Scanned 2024-07-14 2024-07-18 2024-07-16 2024-07-13	(4) (4) (4) (4) (4) (4) (4) (4) (4) (4)	<b>Type</b> Win32 EXE Win32 DLL Win32 EXE Win32 DLL	11dbc8b1503fcf6e021f48acb9e7cb66fb7db3a92b033080ecce2417a0f8807b.exe Updating.dll Defender.exe CleanUp.dll		
codeforprofessiona Communicating Fi Scanned 2024-07-14 2024-07-18 2024-07-16 2024-07-13 2024-07-20	users.com         6 / 92           es (8) ©         Detections           29 / 74         22 / 73           34 / 73         36 / 68           8 / 69         69	<b>Type</b> Win32 EXE Win32 DLL Win32 EXE Win32 DLL Win32 EXE	11dbc8b1503fcf6e021f48acb9e7cb66fb7db3a92b033080ecce2417a0f8807b.exe Updating.dll Defender.exe CleanUp.dll Defender.exe		
codeforprofessional Communicating Fi Scanned 2024-07-14 2024-07-18 2024-07-18 2024-07-13 2024-07-0 2024-07-18 2024-07-18 2024-07-16	users.com         6 / 92           les (8) ©         0           Detections         2 / 74           22 / 73         34 / 73           38 / 68         8 / 69           42 / 72         2	Type Win32 EXE Win32 DLL Win32 DLL Win32 DLL Win32 EXE Win32 EXE	11dbc8b1503fcfGe021f48acb9e7cb66fb7db3a92b033080ecce2417a0f8807b.exe Updating.dll Defender.exe CleanUp.dll Defender.exe 8b970d687ee3b67b4a649df14fea7170N.exe		
ccdeforprofessiona Communicating Fi 2024-07-14 2024-07-18 2024-07-18 2024-07-13 2024-07-20 2024-07-18 2024-07-18 2024-07-18 2024-07-18 2024-07-13	users.com         6 / 92           tes (8) O         O           Detections         29 / 74           22 / 73         34 / 73           38 / 68         8 / 69           42 / 72         11 / 74           45 / 74         65 / 74	Type Win32 EXE Win32 DLL Win32 EXE Win32 EXE Win32 EXE Win32 EXE Win32 EXE	11dbc8b1503fcf6e021f48acb9e7cb66fb7db3a92b033080ecce2417a0f8807b.exe Updating.dll Defender.exe CleanUp.dll Defender.exe 8b970d687ee3b67b4a649df14fea7170N.exe Updating.dll		
codeforprofessiona Communicating Fi Scanned 2024-07-14 2024-07-18 2024-07-18 2024-07-13 2024-07-13 2024-07-20 2024-07-18	4/92           Les (8) O           Detections           29 /74           22 /73           34 /73           36 /68           8 /69           42 /72           11 /74           45 /74	Type Win32 EXE Win32 DLL Win32 EXE Win32 EXE Win32 EXE Win32 EXE Win32 EXE	11dbc8b1503fcf6e021f48acb9e7cb66fb7db3a92b033080ecce2417a0f8807b.exe Updating.dll Defender.exe CleanUp.dll Defender.exe 8b970d687ee3b67b4a649df14fea7170N.exe Updating.dll	Registrant	

+ 2024-05-12 ENDM, INC. | ENDM,

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.

				${ m C}$ Reanalyze $symp $ Similar $$ More $$
38				
(68) Community Score	CleanUp.dll	e2f313c6bc9a47a760c324	3509660b9edb83ffbd47e3a98b ser-input	Size Last Analysis Date A73.00 KB 7 days ago
Score				
DETECTION D	DETAILS RELATIONS	BEHAVIOR	COMMUNITY 2	
Join our Community	y and enjoy additional cor	nmunity insights and crow	dsourced detections, plus an API key to <b>automate checks.</b>	
Contacted URLs (2)				
Scanned	Detections	Status	URL	
			http://r10.o.lencr.org/	
2024-07-09	0 / 94	200	MFMwUTBPME0wSzAJBgUrDgMCGgUABBRpD+QVZ+1vf7U0RGQGBm8JZv 4/SX4OtA==	wdxcgQUdKR2KRcYVIUxN75n5gZYwLzFBXICEgTvbhi0YAPkd2HPyW
2024-07-15	2 / 94	200	https://codeforprofessionalusers.com/api/connectivity	
Contacted Domains				
Contacted Domains Domain		Created	Registrar	0
	(5) ① Detections			0 0
Domain	(5) ① Detections	Created		o
Domain codeforprofessionalu	(5) ① Detections Isers.com 6 / 92	<b>Created</b> 2024-05-10	Registrar	0
Domain codeforprofessionalu firscountryours.eu	(5) ① seers.com 6 / 92 0 / 92 0 / 92	Created 2024-05-10 2024-06-14	Registrar -	0
Domain codeforprofessionalu firscountryours.eu o.lencr.org	(5) ① seers.com 6 / 92 0 / 92 0 / 92	Created 2024-05-10 2024-06-14 2020-06-29	Registrar -	o
Domain codeforprofessionalu firscountryours.eu o.lencr.org postmastersoriginals	(5) beta beta beta beta beta beta beta beta	Created 2024-05-10 2024-06-14 2020-06-29 2024-05-21	Registrar - - CloudFlare, Inc. -	0
Domain codeforprofessionalu firscountryours.eu o.lencr.org postmastersoriginals r10.o.lencr.org	(5) beta beta beta beta beta beta beta beta	Created 2024-05-10 2024-06-14 2020-06-29 2024-05-21	Registrar - - CloudFlare, Inc. - CloudFlare, Inc.	
Domain codeforprofessionalu firscountryours.eu o.lencr.org postmastersoriginals r10.o.lencr.org Contacted IP address	(5) © sers.com 6 / 92 0 / 92	<b>Created</b> 2024-05-10 2024-06-14 2020-06-29 2024-05-21 2020-06-29	Registrar - - CloudFlare, Inc. - CloudFlare, Inc.	
Domain codeforprofessionalu firscountryours.eu o.lencr.org postmastersoriginals r10.o.lencr.org Contacted IP address IP	(5) © sees.com 6 / 92 0 / 92 0 / 92 1 / 92 0 / 92 9 / 92 sees (5) © Detections	Created 2024-05-10 2024-06-14 2020-06-29 2024-05-21 2020-06-29 Autonomous System	Registrar - - CloudFlare, Inc. - CloudFlare, Inc.	
Domain codeforprofessionalu firscountryours.eu o.lencr.org postmastersoriginals r10.o.lencr.org Contacted IP address IP 139.99.221.140	(5) ○ sers.com 6/92 0/92 0/92 1/92 0/92 0/92 1/92 betections 1/92	Created 2024-05-10 2024-06-14 2020-06-29 2024-05-21 2020-06-29 2020-06-29	Registrar - - CloudFlare, Inc. - CloudFlare, Inc. - CloudFlare, Inc.	
Domain codeforprofessionalu firscountryours.eu o.lencr.org postmastersoriginals r10.o.lencr.org Contacted IP address IP 139.99.221.140 162.19.237.181	(5) ○ sers.com 6/92 0/92 0/92 1/92 0/92 365 (5) ○ Detections 1/92 2/92	Created 2024-05-10 2024-06-14 2020-06-29 2024-05-21 2020-06-29 2020-06-20 200-06-20 200-06-20 200-06-20 200-06-20 200-06-20 200-06-20 200-06-20 200-06-20 200-06-20 200-06-20 200-06-20 200-06-20 200-06-20 200-06-20 200-06-20 200-06-20 200-06-20 200-06-20	Registrar - - CloudFlare, Inc. - CloudFlare, Inc. Country AU FR	

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 <u>book a free demo</u> 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