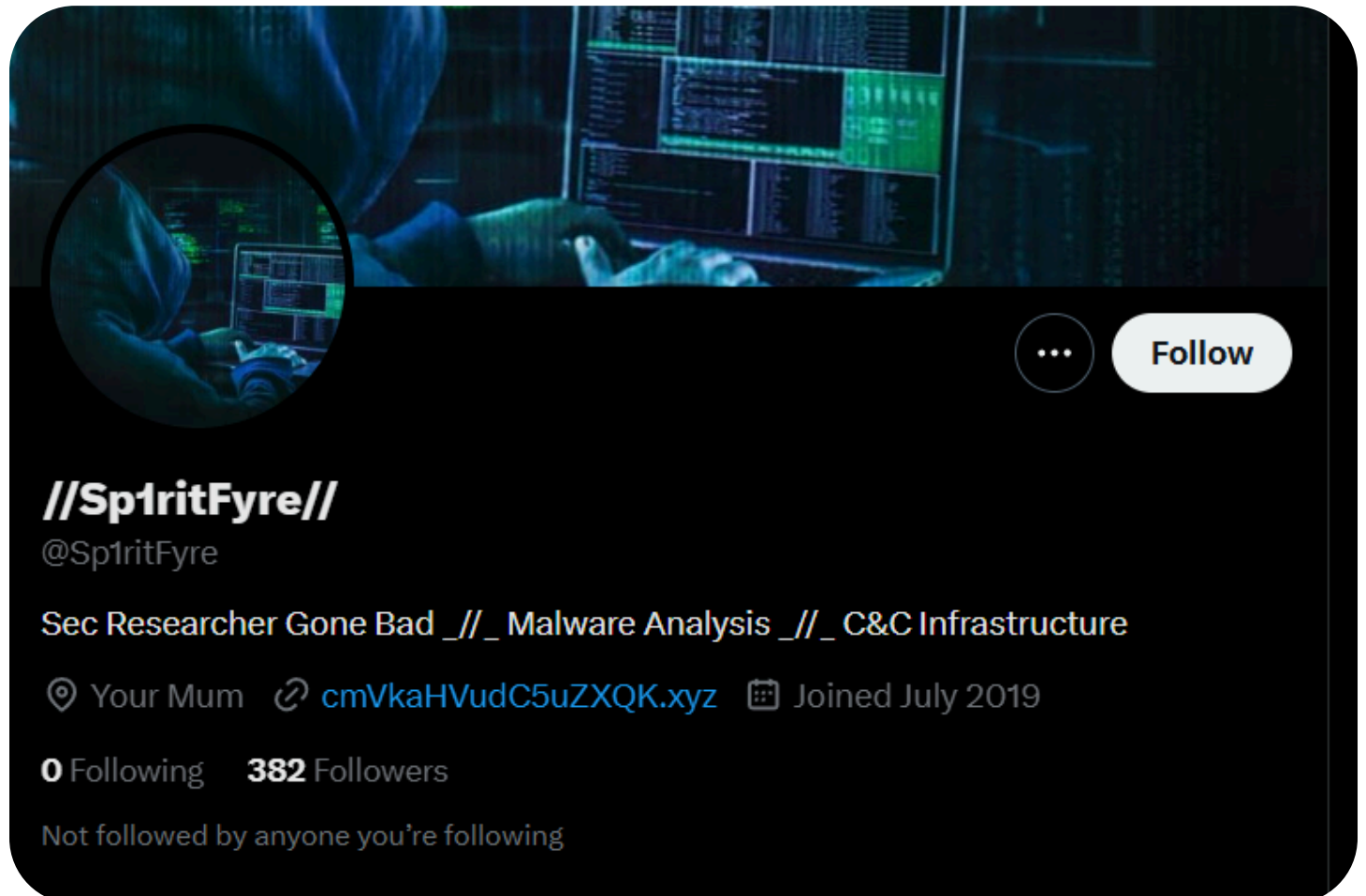


Step-by-Step Reconnaissance:

Twitter Reconnaissance

I accessed the Twitter account of the actor using the handle **@sp1ritfyre**, which my manager had already provided.

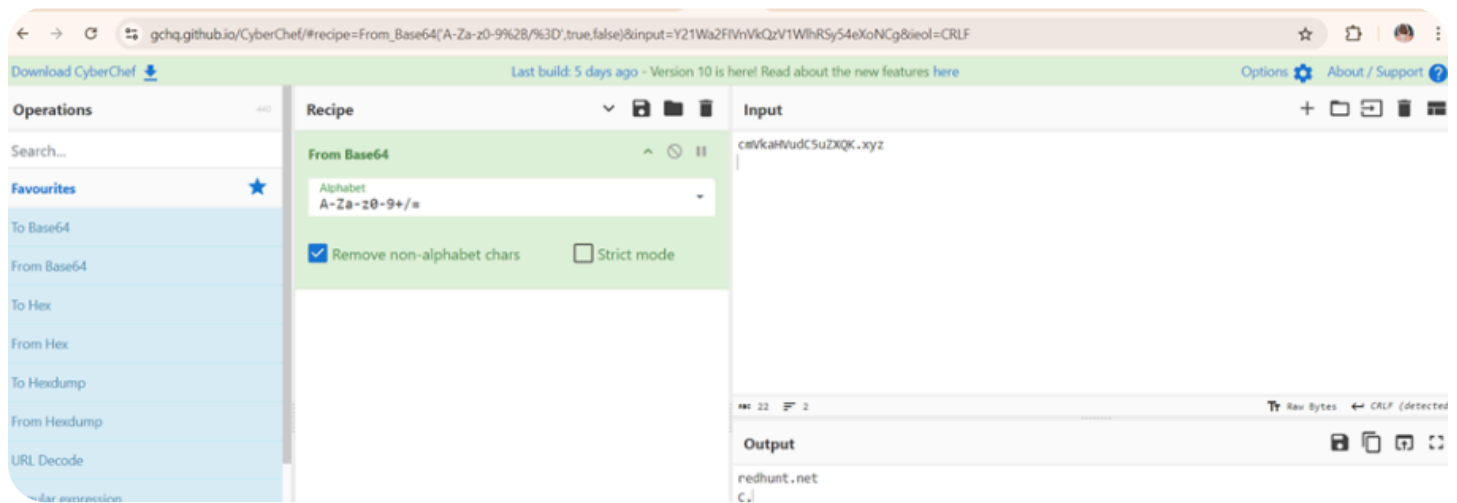


As noted earlier, there was minimal information regarding the malicious actor, apart from a suspected phishing link that seemed to be encoded in **base64**.

Link Decoding

Using CyberChef, an open-source cryptography tool, to decode the Base64 string. The decoded result was a URL:

"**redhunt.net**".



Google Dorks Search

Conducted keyword searches using Google Dorks. The query **"inurl:@sp1ritfyre"** was employed to locate additional social media accounts or websites associated with the POI. I discovered a "Blogger.com" user profile with the same username and profile picture as the Twitter account.

inurl:@sp1ritfyre

AI Mode **All** Images Videos Shopping News Short videos More ▾



Blogger.com

<https://www.blogger.com> › profile ⋮

User Profile: Sp1ritFyre

On Blogger since: March 2020. Profile views: 28,959. Report Abuse. My blogs. Hacker stories. About me. Gender, Female.



Medium · Thato

2 likes · 1 year ago ⋮

Security Blue Team: Introduction to OSINT Capstone.

The first step was to use the information I had, namely the **Twitter/X handle @sp1ritfyre**. While the account itself didn't reveal much ...



LinkedIn · Shukurat Amusa

10+ reactions · 12 months ago ⋮

OSINT CHALLENGE

I navigated to the given twitter account handle of the actor; **@sp1ritfyre**, already provided by my manager. Twitter profile of the POI. As ...



X · Sp1ritFyre

380+ followers ⋮

Sp1ritFyre

@Sp1ritFyre. Sec Researcher Gone Bad __ Malware Analysis __ C&C Infrastructure. Your Mum ...

Navigating the Blog

I examined the blog profile to find more information about the POI.

Sp1ritFyre



[View Full Size](#)

Contact me

[Email](#)

On Blogger since:
March 2020

Profile views: 28,983

[Report Abuse](#)

My blogs

[Hacker stories](#)

About me

Gender Female

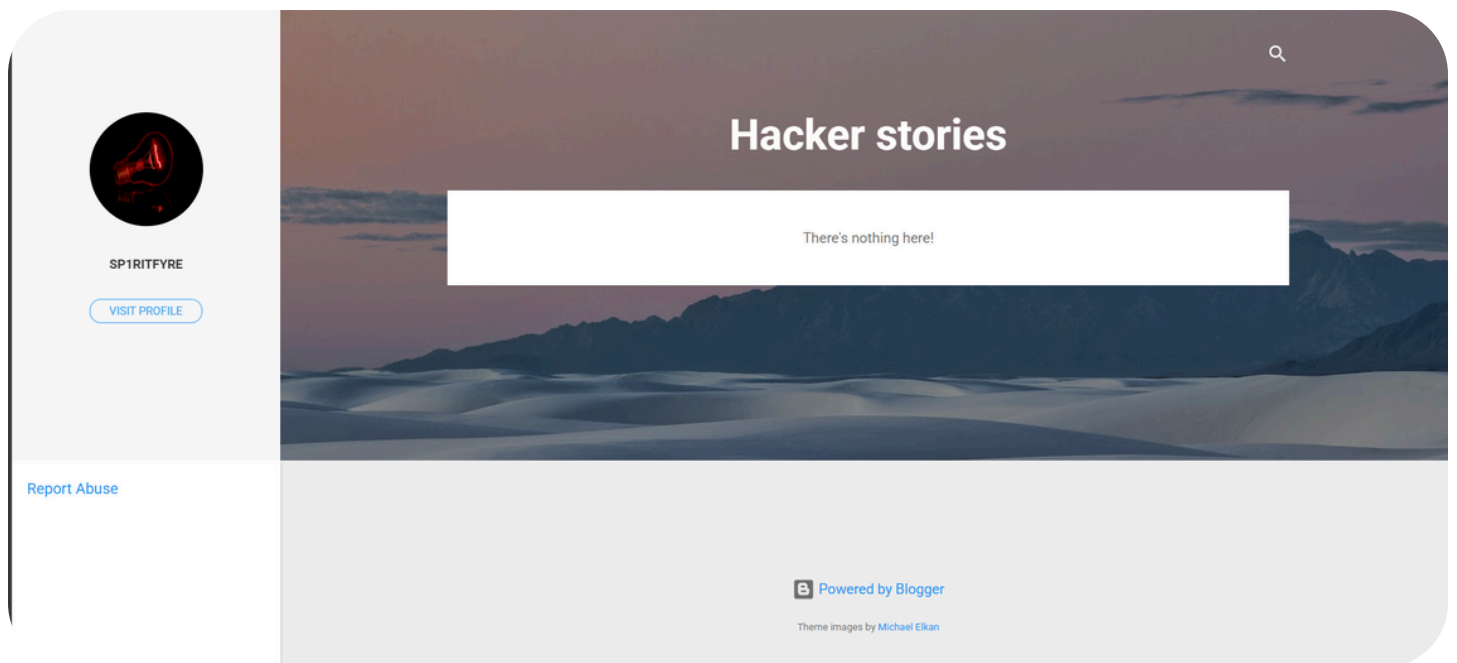
Location 68747470733a2f2f73616d6d6965776f6f647365632e626c6f6773706f742e636f6d

Clicking the **"Email"** in the **"Contact me"** section, I found a personal email address; **"d1ved33p@gmail.com"** and confirmed the user was **female**.

Draft saved

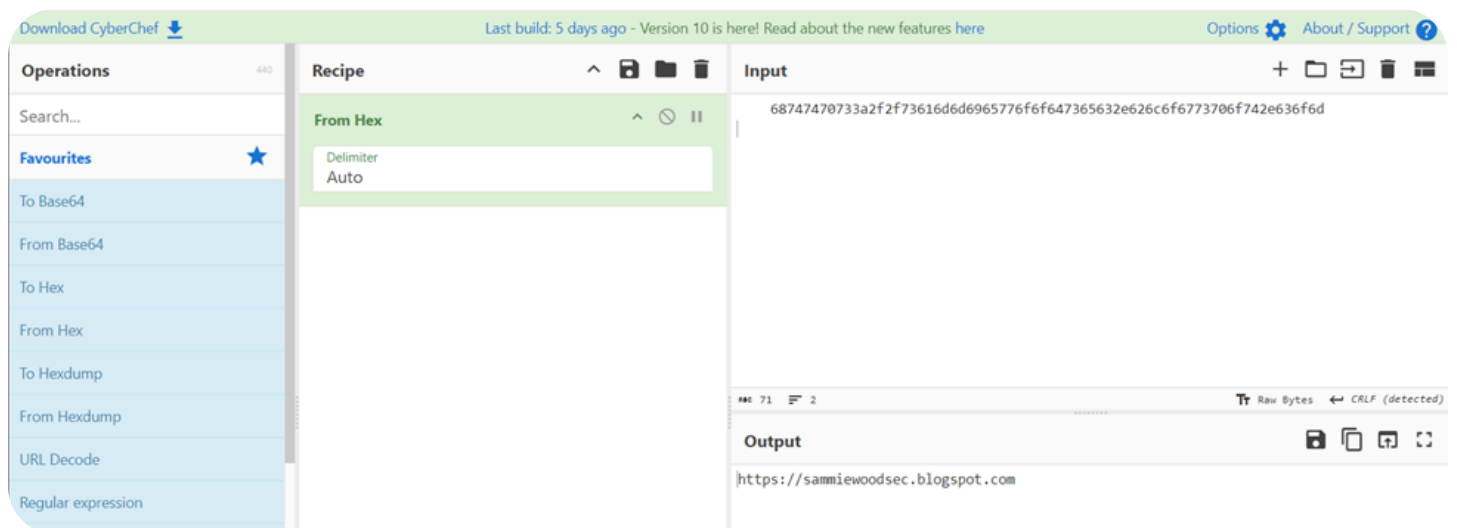
To  d1ved33p@gmail.com X |

Navigating to the **"Hacker stories"** in the **"My Blogs"** section provided a link to a blog post;
"https://sp1ritfyrehackerstories.blogspot.com/".



Location Decoding

Interestingly, I encountered an encoded hexadecimal string in the **"About Me"** section of the Blogger profile, pointing to the location of the hacker. Decoding the hexadecimal string using CyberChef, revealed another blogspot URL: **"https://sammiewoodsec.blogspot.com/"**, potentially registered under the POI's real name.



Further Investigation

Navigating the **"sammiewoodsec.blogspot.com"** blog. Here, additional personal details were uncovered such as real name: **Sam Wood**, Age: **23**. Occupation, interests, and location details were also revealed, confirming the POI's identity.



My blogs

[SamWoodSecurity](#)

About me

[View Full Size](#)

On Blogger since:
June 2019

Profile views: 20,279

[Report Abuse](#)

Gender	Female
Industry	Technology
Occupation	Junior Penetration Tester
Location	Reading, United Kingdom
Introduction	Hey, I'm Sam! Welcome to my profile! Be sure to check out my blog, and if you want to get in touch, email me :)
Interests	Security, Programming, Technology, Gaming, Photography, Camping
Favorite movies	Ready Player One 2018
Favorite music	The Beatles, Rolling Stones, Queen
Favorite books	The Hunger Games series

You moved the pot before the coffee stopped brewing. Do you smell the mountains or the burro?

What the fuck is this about

SamWoodSecurity

Wednesday, July 3, 2019

Wow - my blog is really blowing up!

Thanks to everyone that has been following me, I'm really glad that you find my posts interesting. My post views have been skyrocketing over the past day, and I've been getting a lot of private messages with questions. I can't use my mobile phone at work, but if you need to get in touch, feel free to email my personal address d1ved33p@gmail.com and I'll get back to you ASAP.

With that out of the way, this next blog post is going to be about phishing emails, and how to properly analyse them. I hope this is helpful to some of you wanna-be security researchers out there! (I won't go super deep, you can learn the rest by yourselves)

- [What is a phishing email?](#)
- [How to analyse a phishing email](#)
- [How to analyse a malicious domain](#)
- [How to implement blocks to stop phishing campaigns](#)

In this post, you may see URLs shown like this "google[]com". The square brackets are used to stop the text turning into a hyperlink, making it clickable. This form of sanitisation is to prevent people accidentally clicking on malicious link!

Search This Blog

Pages

[Home](#)

About Me




[SammieWoods](#)

Hey, I'm Sam! Welcome to my profile! Be sure to check out my blog, and if you want to get in touch, email me :)

[View my complete profile](#)

[Report Abuse](#)

How I got into Cyber Security



Hey everyone, my name is Sam, I'm 23, and currently working within the Cyber Security industry. It's an amazing industry that is ever-changing, so no two days are the same! I wanted to share with you my story about how I jumped into this world.

I studied ICT in college, and really enjoyed it. Learning how applications work, how devices talk to each other. It was all crazy. Eventually our course covered a module focus on Security, and despite being very quick and basic, I found myself wanting to know more. I'd spend some free time researching different hacking groups, such as LizardSquad (I remember them taking down Dyn, and DoSing Xbox Live and PSN as a result, pretty cool!) as well as Anonymous, and started reading about state-sponsored groups such as APT 28, and Turla Team.

I went off to University at Plymouth, and studied for a degree in Cyber Security and Forensics. I passed with a 1st degree, and shortly after I started working at PhilmanSecurityInc. I'm currently a junior pen tester, as I realised I preferred breaking stuff (Responsibly!) rather than fixing it.

I love the team here, and both Zach and Dave are great mentors, and constantly help me to develop and expand on my existing skills.

Lots more blog posts coming soon! :)
~ Sammie

Correlating "Redhunt.net"

Going back to my google search query, the next search result correlated with the suspected malicious site decoded from the twitter profile; **"redhunt.net"**. I conducted a domain reputation check and WHOIS lookup using **Cisco Talos Intelligence** and cross verifying with **Domain Dossier**, but no further details were retrieved.

talosintelligence.com/reputation_center/lookup?commit=search&search=redhunt.net#ip-addresses

OWNER DETAILS

DOMAIN redhunt.net

REPUTATION DETAILS

WEB REPUTATION ? Unknown [Submit Web Reputation Ticket](#)

CONTENT DETAILS

CONTENT CATEGORY No established content categories

Think these category details are incorrect?

[Submit Content Categorization Ticket](#)

BLOCK LISTS

TALOS SECURITY INTELLIGENCE BLOCK LIST

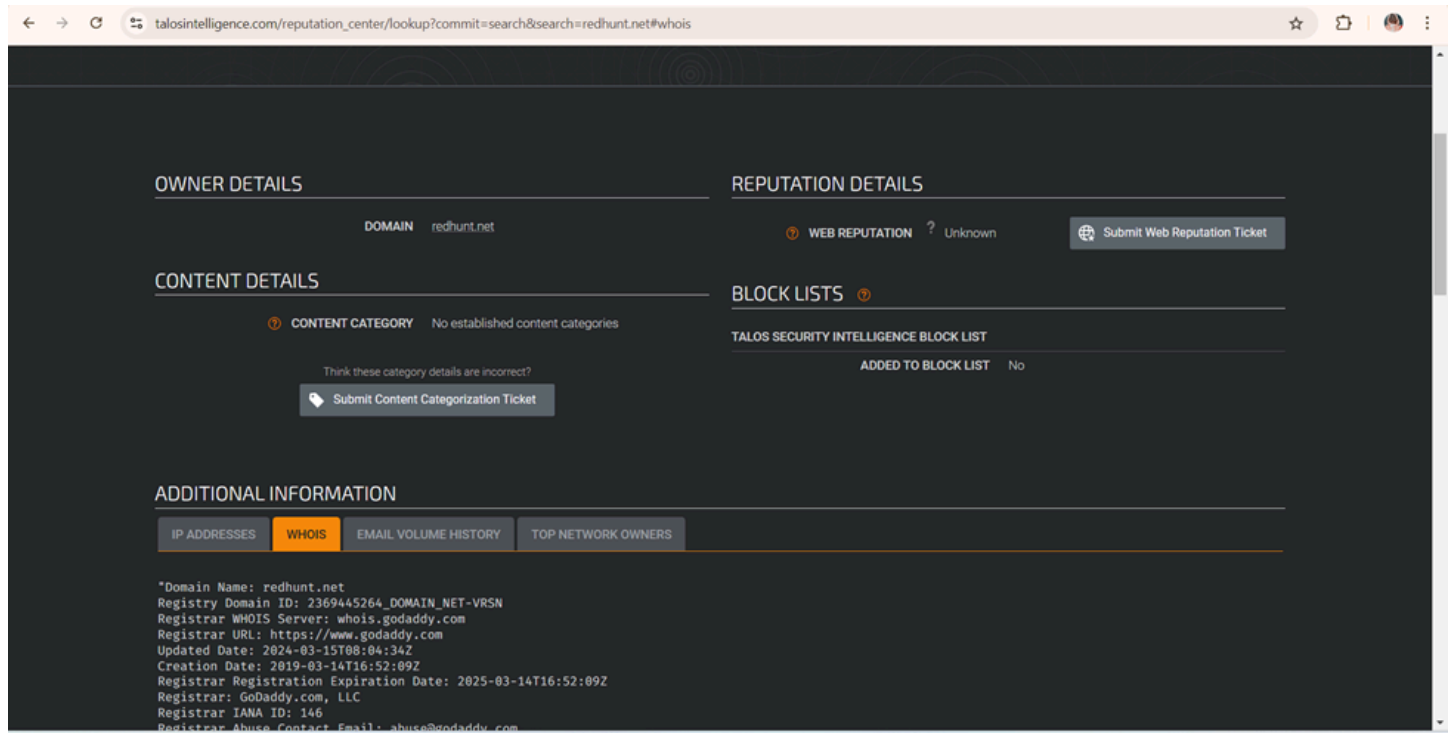
ADDED TO BLOCK LIST No

ADDITIONAL INFORMATION

IP ADDRESSES WHOIS EMAIL VOLUME HISTORY TOP NETWORK OWNERS

Top IP Addresses used to send emails in redhunt.net

IP ADDRESS	HOSTNAME	FWD/REV DNS MATCH	LAST DAY VOL.	LAST MONTH VOL.	BLOCK LISTS	EMAIL REP.
No related IP address data could be found.						



Conclusion:

The investigation effectively uncovered multiple social media accounts and websites associated with the person of interest. It confirmed personal details and indicated potential malicious activities. While some leads did not produce additional information, sufficient evidence was collected to meet the objectives specified in the provided challenge report template.

[1] First Name: Sam

[2] Last Name: Woods

[3] Age: 23

[4] Country: United Kingdom

[5] Interests (5 minimum): Security, Programming, Technology, Gaming, Photography, Camping, Malware Analysis

[6] Hacker's employer (company name): PhilmanSecurityInc

[7] Hacker's position within company: Junior Penetration Tester

Online Presence:

=====

[8] Self-Owned Website (Hacker owns the domain):

"https://redhunt.net"

[9] Other Websites (Person does not own the domain, such as blogs): "https://sp1ritfyrehackerstories.blogspot.com"

"https://sammiewoodsec.blogspot.com"

End of report – submitted for review and further action as deemed appropriate.