OSINT CHALLENGE

Objectives:

- Identify any social-media accounts or websites used by the person-of-interest
- Build up a profile of the person-of-interest
- Find any evidence of malicious behaviour

SCENARIO

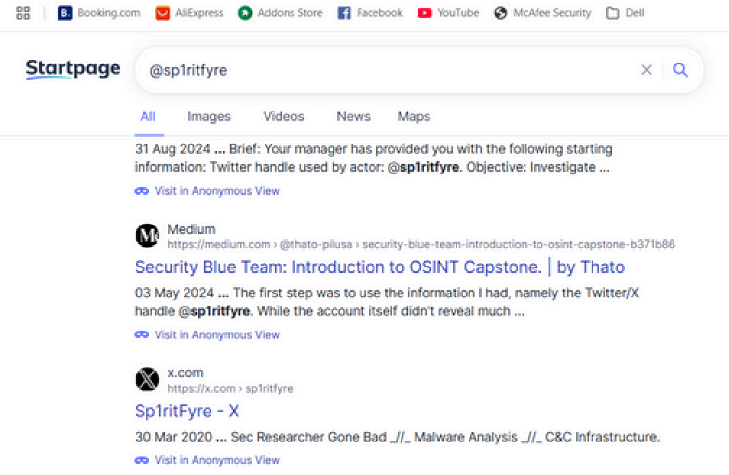
You work for a law enforcement organisation, and you have been assigned to track a person-of-interest, that is believed to be associated with a hacking group that recently compromised a Managed Service Provider (MSP) and are trying to sell the stolen credentials on both the clear net and dark web. Another team is focusing on the dark web lead, so you have been tasked with using OSINT sources to build up a profile on the individual and attempt to locate any evidence that links them to the MSP breach and sale of account details. You have been provided with some information to start your investigation. You should use any of the sources or tools taught in this course, that you deem to be applicable and appropriate.

Your manager has provided you with the following starting information:

- **Twitter handle used by actor:** @sp1ritfyre

1. First Look: The Twitter Profile

I started my investigation by searching for the Twitter name @sp1ritfyre on Google. My goal was to find any public information about this person online. I successfully found the Twitter profile for @sp1ritfyre. However, when I looked at the profile, there was no personal information that could help me figure out who this person was.



@sp1ritfyre

31 Aug 2024 ... Brief: Your manager has provided you with the following starting information: Twitter handle used by actor: **@sp1ritfyre**. Objective: Investigate ...

Visit in Anonymous View

Medium
https://medium.com › @thato-pilusa › security-blue-team-introduction-to-osint-capstone-b371b86

Security Blue Team: Introduction to OSINT Capstone. | by Thato

03 May 2024 ... The first step was to use the information I had, namely the Twitter/X handle **@sp1ritfyre**. While the account itself didn't reveal much ...

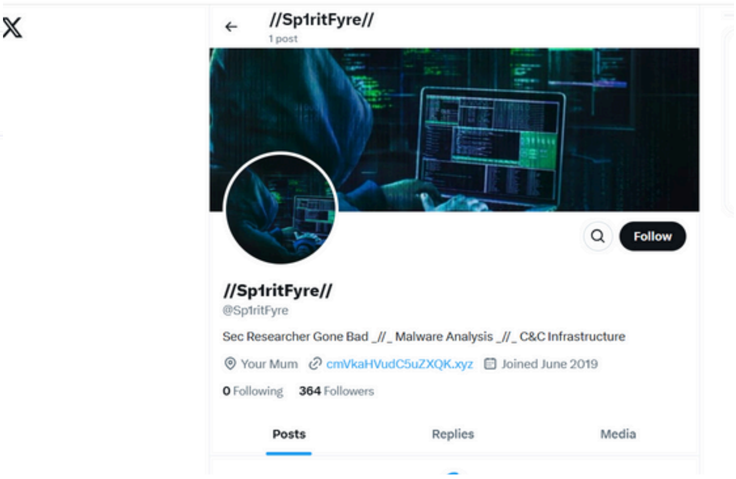
Visit in Anonymous View

x.com
https://x.com › sp1ritfyre

Sp1ritFyre - X

30 Mar 2020 ... Sec Researcher Gone Bad _//_ Malware Analysis _//_ C&C Infrastructure.

Visit in Anonymous View



//Sp1ritFyre//
1 post

//Sp1ritFyre//
@Sp1ritFyre

Sec Researcher Gone Bad _//_ Malware Analysis _//_ C&C Infrastructure

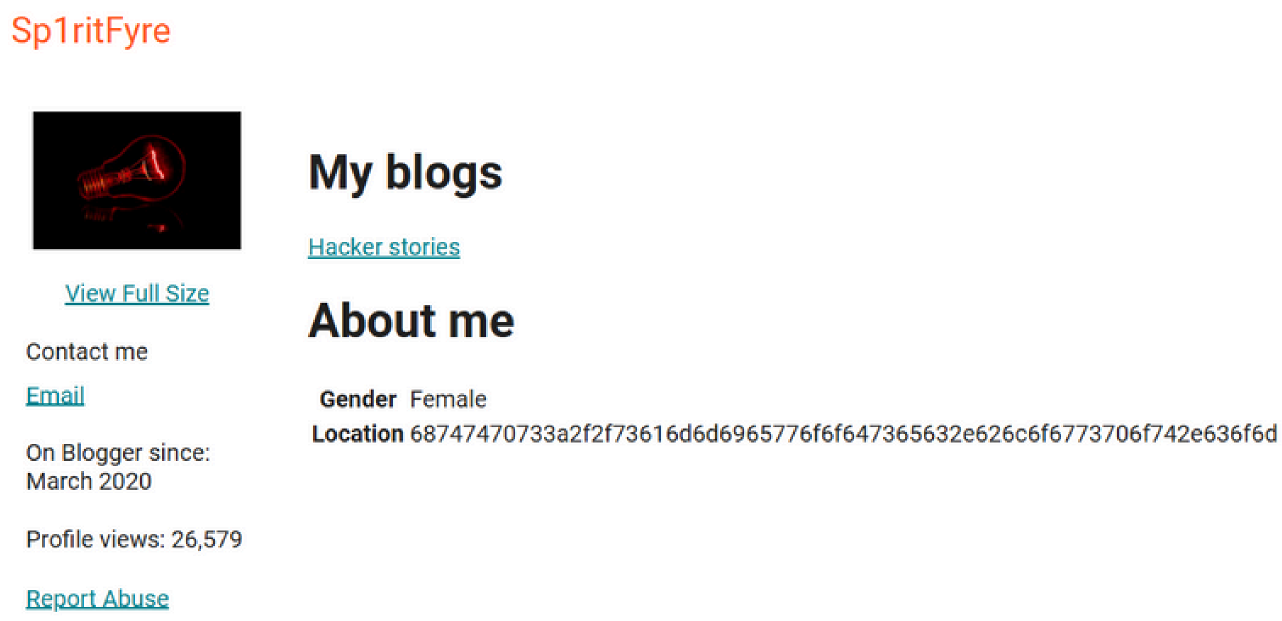
Your Mum cmVkaHVudC5uZXQK.xyz Joined June 2019

0 Following **364** Followers

2. Finding a Hidden Link

As I kept looking through the search results, I found a strange link. It looked like cmVkaHVudC5uZXQK.xyz. I clicked on this link, and it took me to a webpage made with Blogger. This was an important step because it showed the person had an online presence beyond just Twitter. What I Saw on the First Blogger Page

On the first Blogger page, there wasn't much information. It only mentioned a gender and had a long string of letters and numbers, a hexadecimal code, where a location would normally be. This told me the hexadecimal code was important and needed to be looked at closely.



Sp1ritFyre

View Full Size

Contact me

Email

On Blogger since:
March 2020

Profile views: 26,579

Report Abuse

My blogs

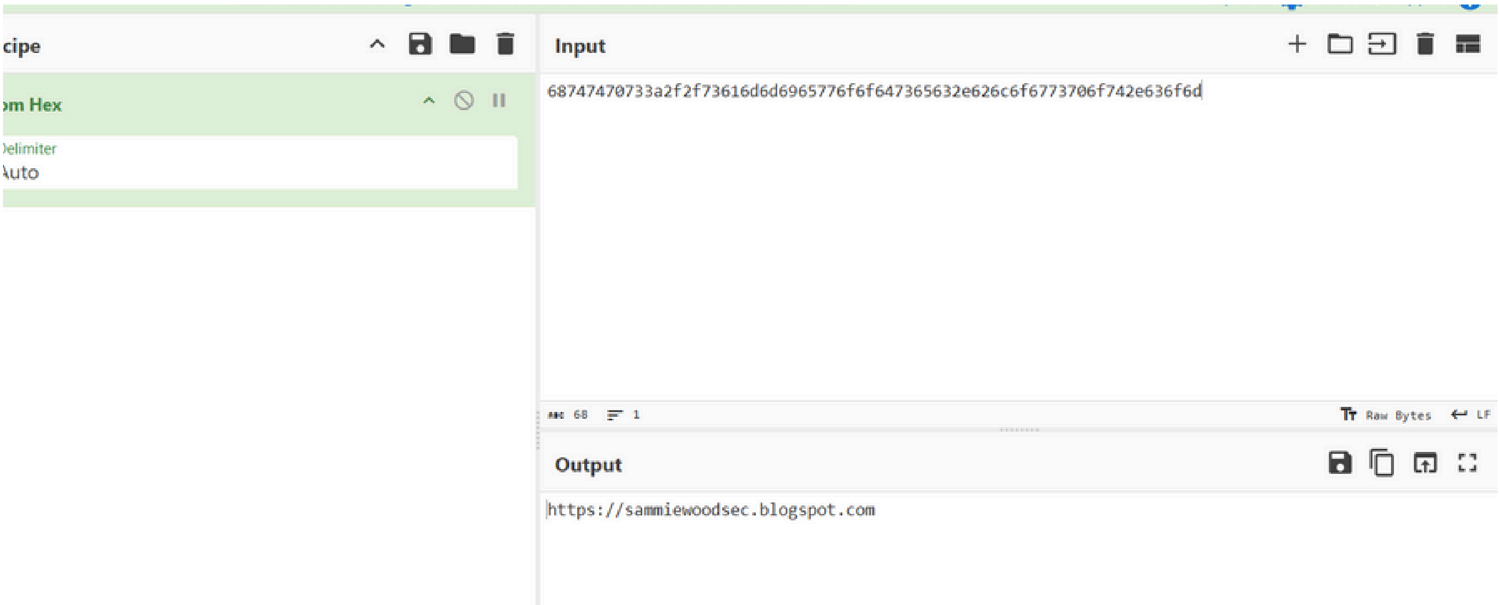
Hacker stories

About me

Gender Female
Location 68747470733a2f2f73616d6d6965776f6f647365632e626c6f6773706f742e636f6d

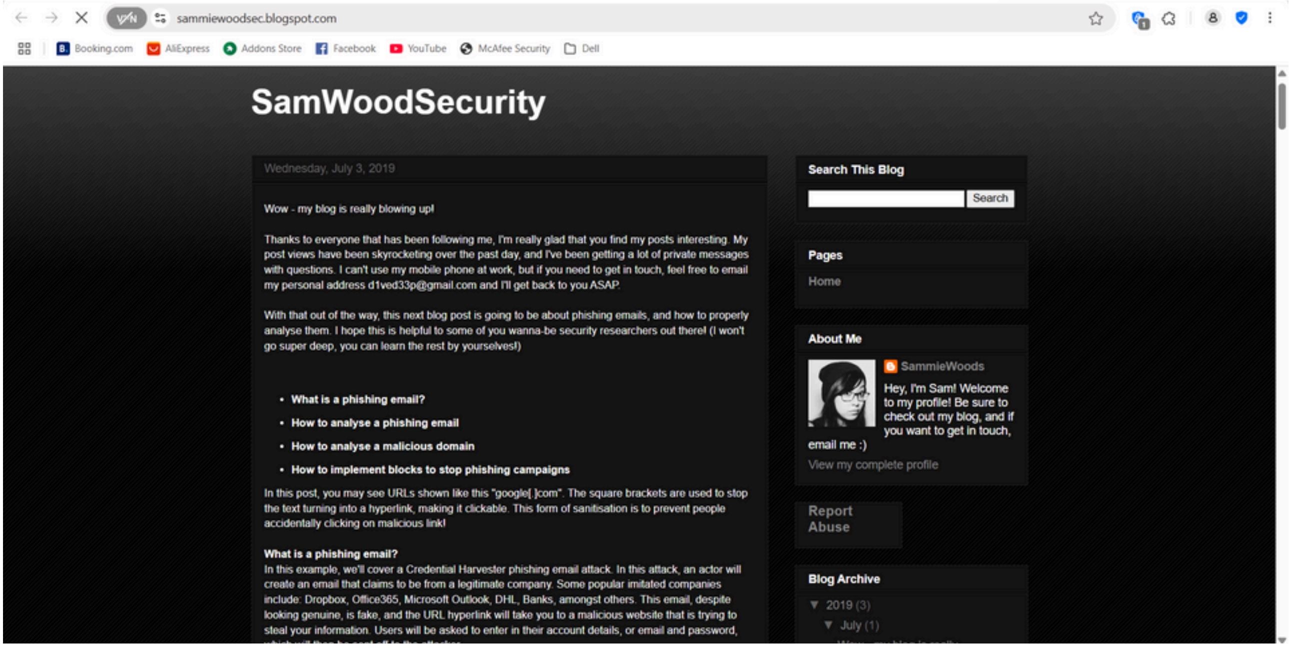
3. Decoding and Discovering the Main Blog

I used a tool called CyberChef to understand what the hexadecimal code meant. It turned out it wasn't a location at all. Instead, it was a web address (URL) for another Blogger site. When I went to this new site, I found a blog that had a lot of the information I needed about the person.



```
68747470733a2f2f73616d6d6965776f6f647365632e626c6f6773706f742e636f6d
```

```
https://sammiewoodsec.blogspot.com
```



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**

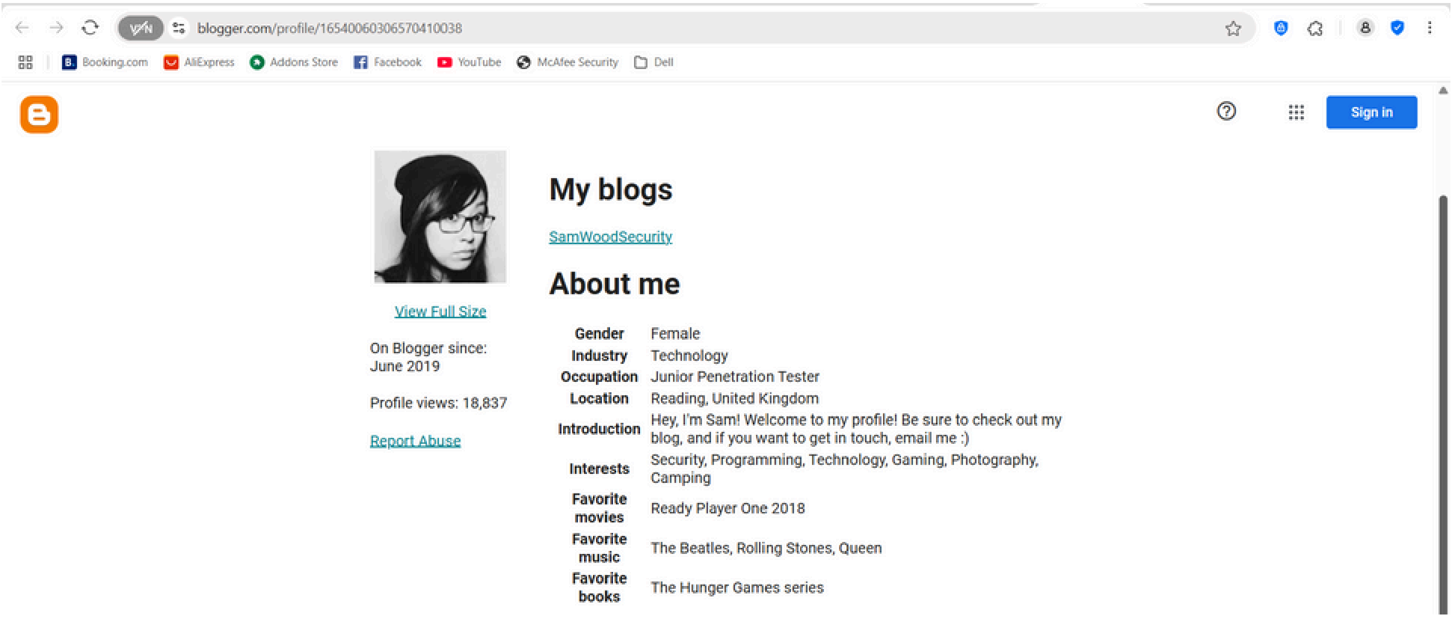
In this post, you may see URLs shown like this "google[.]com". The square brackets are used to stop the text turning into a hyperlink, making it clickable. This form of sanitisation is to prevent people accidentally clicking on malicious link!

What is a phishing email?
In this example, we'll cover a Credential Harvester phishing email attack. In this attack, an actor will create an email that claims to be from a legitimate company. Some popular imitated companies include: Dropbox, Office365, Microsoft Outlook, DHL, Banks, amongst others. This email, despite looking genuine, is fake, and the URL hyperlink will take you to a malicious website that is trying to steal your information. Users will be asked to enter in their account details, or email and password,

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 :)

4. Getting All the Details: Sammie Woods's Profile

On this second blog, there was an option to "view complete profile." I clicked this, and it led me to another page with even more details. This allowed me to gather all the important information about our person of interest.



View Full Size

On Blogger since:
June 2019

Profile views: 18,837

Report Abuse

My blogs

SamWoodSecurity

About me

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

Here is what I found about them:

- First Name: Sammie
- Last Name: Woods
- Age: 23
- Country: United Kingdom
- Interests: Sammie Woods is interested in Security, Programming, Technology, Gaming, Photography, and Camping.
- Employer: Philman Security Inc
- Job: Junior Penetration Tester.
- Their Own Website: https://redhunt.net
- Other Websites: https://blogger.com (This is where the blog profile was.)
- Email Address: d1ved33p@gmail.com.

This detailed information about Sammie Woods, including their job and online activities, gives us a lot of useful clues for our investigation into the computer system breach and the selling of account details.