

Introduction to OSINT

Challenge Submission

Challenge Scenario

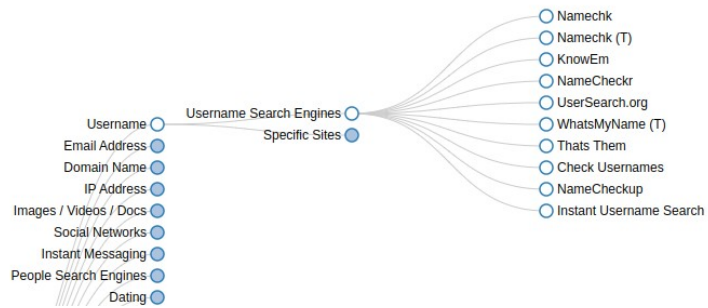
You work for a law enforcement organisation, and you have been assigned to track a person-of-interest, that is believed to be associated with a hacking group that recently compromised a Managed Service Provider (MSP) and are trying to sell the stolen credentials on both the clear net and dark web. Another 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. We know that the email address used to register the Twitter account is fake, so do not include this in your report.

Challenge Resources

Your manager has provided you with the following starting information: Twitter handle used by actor: @sp1ritfyre .You can download a list of the information you have been asked to retrieve about the subject (.txt file). You should use this to help you find the right information, ready to hand in during the Challenge Submission in the next lesson. This will help to keep you on track, and not gather information that is not relevant to the current investigation. See the “Tips and Advice” section below before starting.

Try using OSINT framework tool to check to more about the given user handle. You can use the instant username search tool. We found the same username is in facebook. But it's seems to removed. Check the twitter account. It has a link and encoded. Analyze the text using online analyzer and it's found base64 was used for encoding. After decoding it, the link is found to be redhunt.net (Remove the .xyz extension while analyzing and decoding)

OSINT Framework



Instant Username Search

sp1ritfyre

Instagram

Available

TikTok

Available

Twitter

Taken

Facebook

Taken

YouTube

Available

Medium

Available

Reddit

Available

HackerNews

Taken

GitHub

Available

Quora

Available

9GAG

Available

VK

Available

GoodReads



Available


Blogger

Available


Patreon

Available

 Settings






//Sp1ritFyre//
1 post




//Sp1ritFyre//
@Sp1ritFyre

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

 Your Mum  cmVkaHVudC5uZXQK.xyz  Joined July 2019

0 Following 205 Followers


PostsRepliesMediaLikes




//Sp1ritFyre// @Sp1ritFyre · Mar 30, 2020
If you know, you know

...

Also try searching the username in the search engines. Will get a blog with the given username.





[All](#)
[Images](#)
[Videos](#)
[News](#)
[Maps](#)
[Settings](#)

☐ India (en)
 ☐ Safe search: moderate
 ☐ Any time

<https://twitter.com/sp1ritfyre>
[//Sp1ritFyre// \(@Sp1ritFyre\) / Twitter](#)
 The latest tweets from [@sp1ritfyre](#)

<https://twitter.com/Sp1ritFyre/status/1244545810878148609>
[@Sp1ritFyre | Twitter](#)

https://twitter.com/Sp1ritFyre/with_replies
[Tweets with replies by //Sp1ritFyre// \(@Sp1ritFyre\) / Twitter](#)
 Sec Researcher Gone Bad _//_ Malware Analysis _//_ C&C Infrastructure. Your Mum
 cmVkaHVudC5uZXQK.xyz Joined June 2019. 0 Following. 138 Followers. Tweets. Replies. Media.

<https://www.blogger.com/profile/08313689826885886832>
[Blogger: User Profile: Sp1ritFyre](#)
 Sp1ritFyre. View Full Size. Contact me. Email. On Blogger since March 2020. Profile views - 9408.

Sp1ritFyre



[View Full Size](#)

Contact me

[Email](#)

On Blogger since
March 2020

Profile views - 9441

My blogs

[Hacker stories](#)

About me

Gender	Female
Location	68747470733a2f2f73616d6d6965776f647365632e626c6f6773706f742e636f6d

Will see the location value encoded. So we need to find what algorithm was used to encode the the original value. Using the help of online encoder identifier we can find it is encoded in hexadecimal. Now convert the hexadecimal value to ASCII value using any converter available online. This will lead to the hacker's original blog where all the the questions will be answered.

Analysis Results

68747470733a2f2f73616d6d6965776f6f647365632e626c6f6773706f742e636f6d

Your ciphertext is likely of this type:

Hexadecimal Code (click to read more)

From

To

Hexadecimal

Text

Open File

Paste hex numbers or drop file

68747470733a2f2f73616d6d6965776f6f647365632e626c6f6773706f742e636f6d

Character encoding

ASCII

Convert

Reset

Swap

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, which will then be sent off to the attacker.

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

Blog Archive

▼ 2019 (3)

▼ July (1)

Wow - my blog is really

SammieWoods



[View Full Size](#)

On Blogger since
June 2019

Profile views - 7508

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

Read through the complete blog, all the questions will be answered. A couple of answers will not be direct, it will be encode in some format, try decoding those.

Check out correct answers here!

[1] First Name: Sammie

[2] Last Name: Woods

[3] Age: 23

[4] Country: United Kingdom

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

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

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

[8] What is the full url of the website owned by the hacker? redhunt.net

[9] List any full URLs of websites not owned, but used by the hacker (Blogs only) Broken question
(Let me know if you got it)

[10] What email address has been used by the hacker? d1ved33p@gmail.com