iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** V **Month of publication:** May 2022

DOI: https://doi.org/10.22214/ijraset.2022.42728

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue V May 2022- Available at www.ijraset.com

Study on How Dark Web Facilitate Cyber Security Experts to Improve Business Security?

Mr. Dinesh Pal[1], Mr. Ankush Pandey[2]
[1, 2]*Thane - Maharashtra*

Abstract: ***The term dark web has been associated with illegal context for good reasons. For a typical web user, the dark web is the digital area wherever medicine, weapons and alternative prohibited things are sold. The dark web is ill-famed for many criminal activities and deals. this is often the overall public image of the dark web.***
But the assumption is totally different for cyber security experts. There are several edges for cyber security experts exploiting the dark web. they'll use the information and insights offered on the dark web to find out additional concerning trending techniques and tricks getting used by hackers
The dark web has been similar to the darknet markets. however, there's an occasion that not everybody is aware of regarding it. The term darknet market is often used for billion-dollar business activities and illicit and illegal activities.
A unique feature of the dark web is the use of cryptography technologies to cover the main points of your business clients' identities, that area unit getting used by criminals in shopping for and merchandising medication, and alternative nonlegal things.

Keywords
- ***Cyber Security***
- ***Dark web***
- ***Internet***
- ***Hackers***
- ***Business Security***

I. OBJECTIVE

1) Improve the security posture of your organization.
2) Right use of this technique and others, cyber security experts can open new doors of opportunities

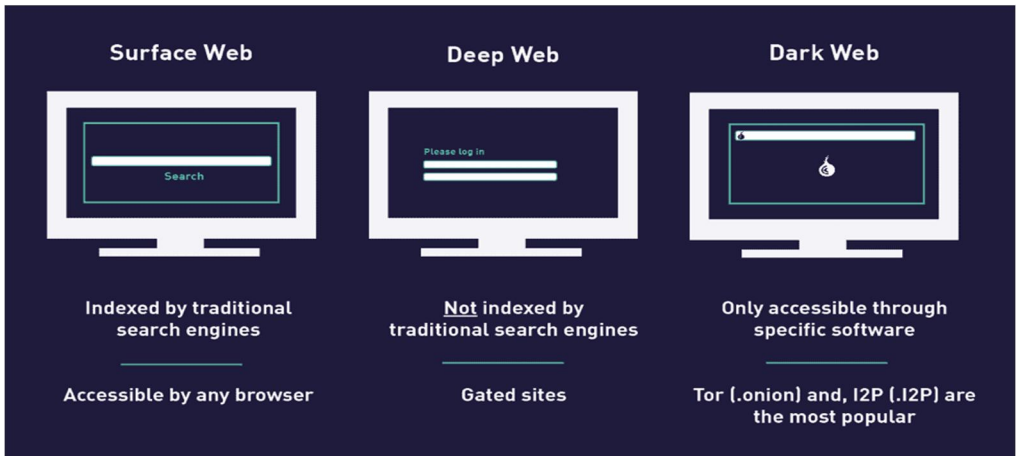
II. INTRODUCTION

The dark web is an internet space. It's been associated with illegal activities. According to the Federal Bureau of Investigation (FBI), there are few exceptions for dark web surfing.

1) The first exception relates to government staff. They can't use the dark web within the workplace or elsewhere while not permission. The second exception relates to work-related enforcement activities.
2) The second exception is related to work enforcement activities. enforcement agencies have the authority to enter any part of the world without saying anything regarding their whereabouts, within their authoritative boundaries. So they can access these areas where the dark web has simply appeared.
3) Cyber security experts in enforcement can use the similar dark web to store data and records till a judicial writ is passed. They can't access an individual's information without a judicial writ. So, they need the authority to access the internet domains of these websites, where illegal activities have been carried out.

The most controversial aspect of this is that enforcement agencies don't need a judicial writ to access any information stored on the dark web. No one aware of whether these agencies are abusing their power in this manner.
However, let's first dispel some misconceptions about the dark web.

a) *Assumption 1 — The Dark Web is Synonymous with the Criminal Internet:* While the dark web is home to lot of crime, it also hosts many legitimate corporations like New York Times and Facebook which offer Tor-based services, as well as typically gentle content. The dark web is not like cybercrime
b) *Assumption 2 — The Dark Web is Similar thing as the Deep Web:* To clarify, the deep web is defined as something that is not indexed by ancient search engines. Unsurprisingly, the deep web is additionally home to criminality. The dark web does not monopolize cybercrime.



Source: digitalshadows.com

III. POTENTIAL SCOPE AND BENEFITS OF DARK WEB FOR CYBER SECURITY EXPERTS

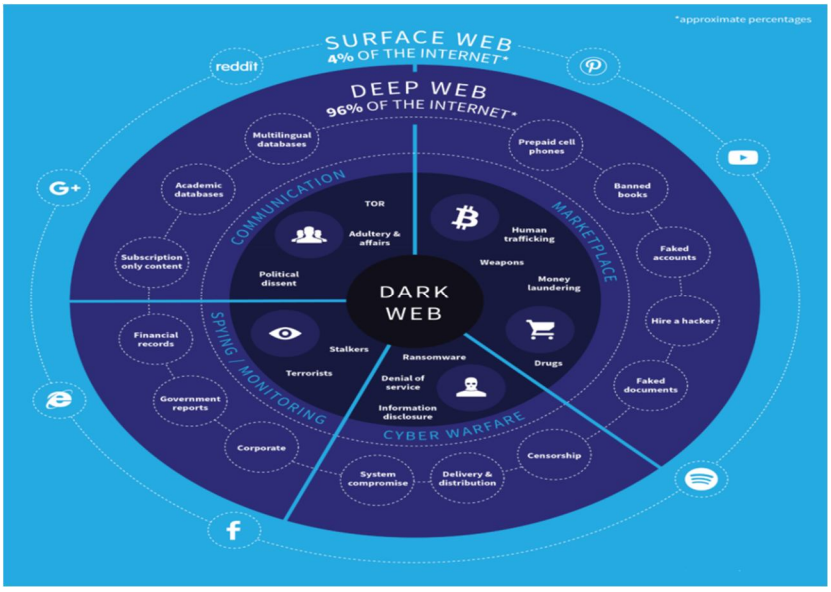
There are a unit several organizations fighting against cyber criminals through the dark web. The dark web provides them with a chance to fight against hackers and cyber spies.

The primary reason for typically the presence of encrypted communication. This involves technology-based communication between two or a lot of people. This is what makes it totally different from other communication ways, which don't use encryption technologies to ensure privacy and data communication security.

IV. DARK WEB SERVICES

The dark web also presents the option of paying for sensitive information and hacking services instead of malware and virus packages that require the buyer to have a higher level of expertise. Security author Matias Porolli lists these services in "Cybercrime Black Markets: Dark Web Services and Their Prices" on WeLiveSecurity.

1) *Ransomware as a Service:* Preconfigured ransomware sold on a monthly or annual basis.
2) *Selling Access to Servers:* Remote desktop protocol (RDP) credentials sold per server through a customizable search service
3) *Renting Infrastructure:* Computing resources leased for botnets and denial-of-service attacks that require massive processing power
4) *Selling PayPal and Credit card Accounts:* Account access credentials sold to cyber criminals for a fraction of the available balance on each account



Sources: ubermetrics-technologies.com

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue V May 2022- Available at www.ijraset.com

V. WHY MUST ORGANIZATIONS CARE ABOUT THE DARK WEB?

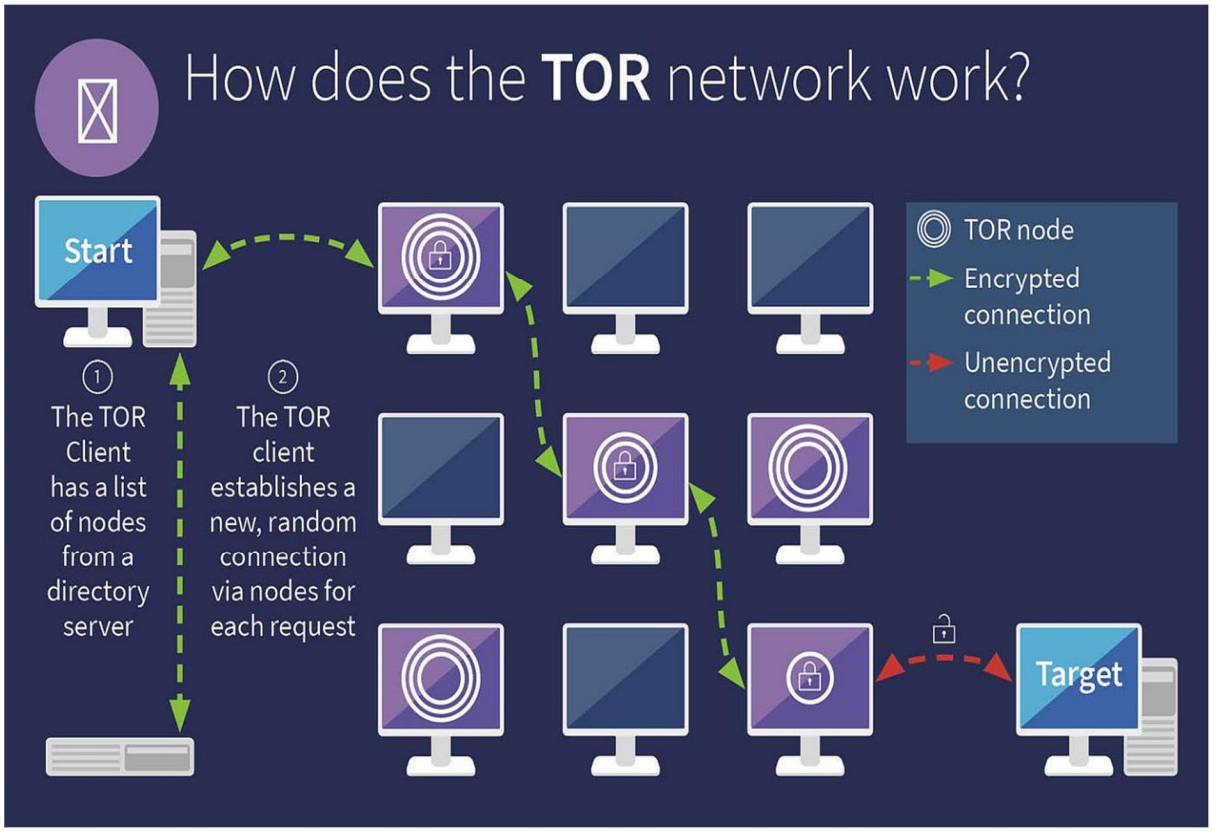
It's now become one of the most popular topics in cyber security. because it has emerged as one of the most important security threats in recent years.

Cyber security experts are always tracking the activities during this digital space to get an idea regarding the next big cyber-attack. These cyber-attacks can occur in any country. So, it's essential to know about them, because there are millions of people who are at risk around globe.

What's fascinating is that the dark web has become one of the busiest places for hackers to do their illegal activities, alternative to other favourite places like the deep web, TOR network, and i2p network. The reason for its popularity is its ability to cover a user's identity. This can be achieved using robust encryption methodology.

All these characteristics make it an ideal place for hackers. So, they've been using the dark web as a base from which to launch attacks worldwide.

Here's a TORFlow from Uncharted Software, showing data flow throughout the TOR network.



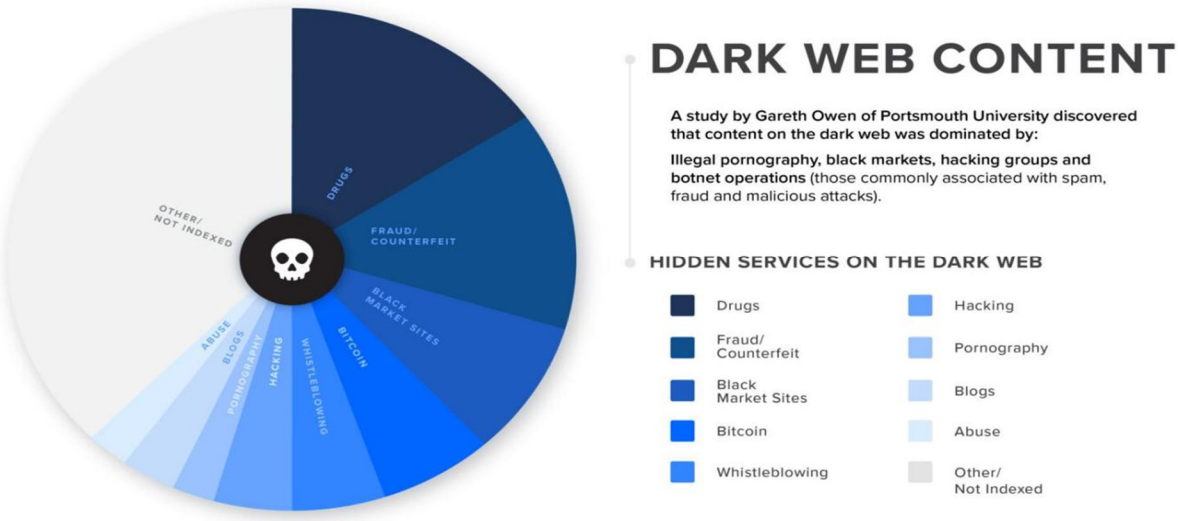
Sources: gdata-software.com

VI. WHY DO CYBER SECURITY EXPERTS FOCUS ON DARK WEB?

While browsing the regular internet, users can access all kinds of content and information from any website. But when it comes to dark web surfing, you can simply access illegal content from sites selling illegal drugs, weapons, malware, and other banned items. These sites are spread worldwide. And everyone tries to stay away from them because they're using encryption methodology to hide identities

Cyber security experts are trace1 various criminal activities happening on these sites. And these may take place at a similar time in several countries worldwide. The primary reason for this is the sophisticated use of encryption technologies, which provide a safeguard to protect sensitive information communication.

There's a lot of content on the dark web not available on the regular internet. For instance, there are plenty of sites in various countries where people can buy and sell weapons and drugs in exchange for cryptocurrencies. There are also sites in many countries that sell fake passports, IDs, and other false documents, which can help with identity protection.



Source: sstech.us

VII. 8 WAYS CYBER SECURITY EXPERTS BENEFIT FROM DARK WEB

To tackle business threats by hackers, it's important to know how hackers and exploiters operate. There's no better place than the dark web to interact with hackers. The dark web is not only meant for cyber criminals, but also cyber security experts can use this to improve business security.

Hackers who want to exploit your organization always use the dark web to publish stolen data so active cyber security experts can easily track business information available for sale by hackers. A proactive approach is using the dark web to save your organization from major security setbacks. It's best to use the dark web to improve your security posture.

Here are 8 ways cyber security experts benefit from dark web and improve business security.

A. Gather Threat Intelligence

Dark web surfing is never silent. There's continually chatter about possible threats and major cyber security threats by hacking teams. Associating with the right group can help you gain data that can be helpful for your organization.

As a security analyst, you'll be able to ready to tackle possible security attacks with information gathered from the dark web. You can get data about the potential attack vector and the mitigation tactics of such attacks. You will also learn some new methods about how to handle security threats by talking to hackers and getting any relevant data about their operations.

B. Hear Information from Hackers

Hacking group members will share important data related to their operations and hacking tools they use. You able to collect this intelligence and thoroughly analyze it so you can prevent similar attacks.

Cyber security experts also need to know how these hackers work so no risks can be created in your business systems. Knowing the details about the hackers' operations will be useful for you to take the necessary steps to enhance your business security.

C. Protect Information from Hackers

There are various means by which legitimate organizations can secure themselves from hackers. These hackers may also try to get sensitive data from an organization by hacking its systems.

You cannot prevent such attacks. But you can protect your valuable data from being accessed by cybercrime.

There are certain measures you can adopt to protect sensitive data from being stolen—and letting this data be used for illegal purposes—through a comprehensive end-to-end security roadmap, which includes monitoring, detection and managing threats.

The dark web can help you apply cyber security shields for your organization's data. This will help reduce security threats imposed by hackers.

D. Protect Users' Privacy

Whenever you're using the internet, you're making yourself target for hackers. You're not only exposed to cybercrime, but also sharing your confidential information with various government agencies, keeping track of user activities across the internet.

It's important to understand how these agencies can trace user activities. You can do this by Gathering certain information about their online behaviour.

You need to secure yourself from ISPs and other local network members, so your classified data is still safe. Strong privacy protection can help you secure sensitive business data. And this will be useful for enhance your business security and minimizing security threats.

E. Protect Business Data

Another way to secure your organization's data through the dark web is checking on your employees unintentionally sharing your business data on the internet.

By actively surfing the dark web, security experts can mitigate the chances of a data breach by removing the business information.

F. Protect Intellectual Property

Hackers try to get data about the intellectual properties of organizations. This may involve any patent, signed agreement, research details and clinical data.

It's difficult for a hacking group to get such valuable data. But the group can get details by using its own techniques.

There are also other ways cyber criminals can easily find these business secrets. Innovative ideas of organizations should be under lock and key, so it doesn't get taken by dark hackers.

G. Prevent Data Being Exposed on the Internet

You must always secure your organization's data from the public view. Else, it can lead to several types of attacks against your business systems.

By actively surfing the dark web, security experts can mitigate the chances of a data breach by removing the business information.

H. Protect Login Credentials

You will learn how to handle the login credentials of users through the dark web . Often, users do not protect their usernames and passwords, making them easy for cyber attack. Hackers use phishing emails to steal sensitive data about users' login details.

It's important to educate users about such attacks. Teach them how they can reduce the chances of their login credentials being stolen by hackers.

VIII. HOW ORGANIZATIONS IMPROVE SECURITY BY MOVING TO DARK WEB

Some organizations are building sites on the dark web to enhance their security posture. Doing so this can make it harder for mainstream users to visit sites like Amazon and Facebook. These examples of organizations with dark web sites are used to secure their users from cyber criminals, marketing companies and governments tracking user information.

It also allows peoples to access platforms in other countries, such as China, Cuba and North Korea, that block networks.

Many organizations in the private sector are even using their own dark web site to remove themselves from potential hackers. Many organizations are shifting to the dark web after migrating to the cloud but found themselves within the centre of attention of bad actors.

So, they decided more security for their organization, clients or customers was needed.

Moving to the dark web can also be an excellent tool for promoting. Marketers can use the dark web to realize insights into potential needs and wants of current or future clients by reading vast amounts of completed online forms.

As more companies move to the dark web, old marketing strategies will be affected. That's because marketers will be unable to get effective data to tap customers. And analytics will then be less accurate due to more consumers using TOR browsers and different hidden networks.

marketers must use caution when using the dark web. It's filled with lots of sensitive, criminal and sensitive data, which can cause effect to both an organization and employee brand images.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue V May 2022- Available at www.ijraset.com

IX. CONCLUSIONS

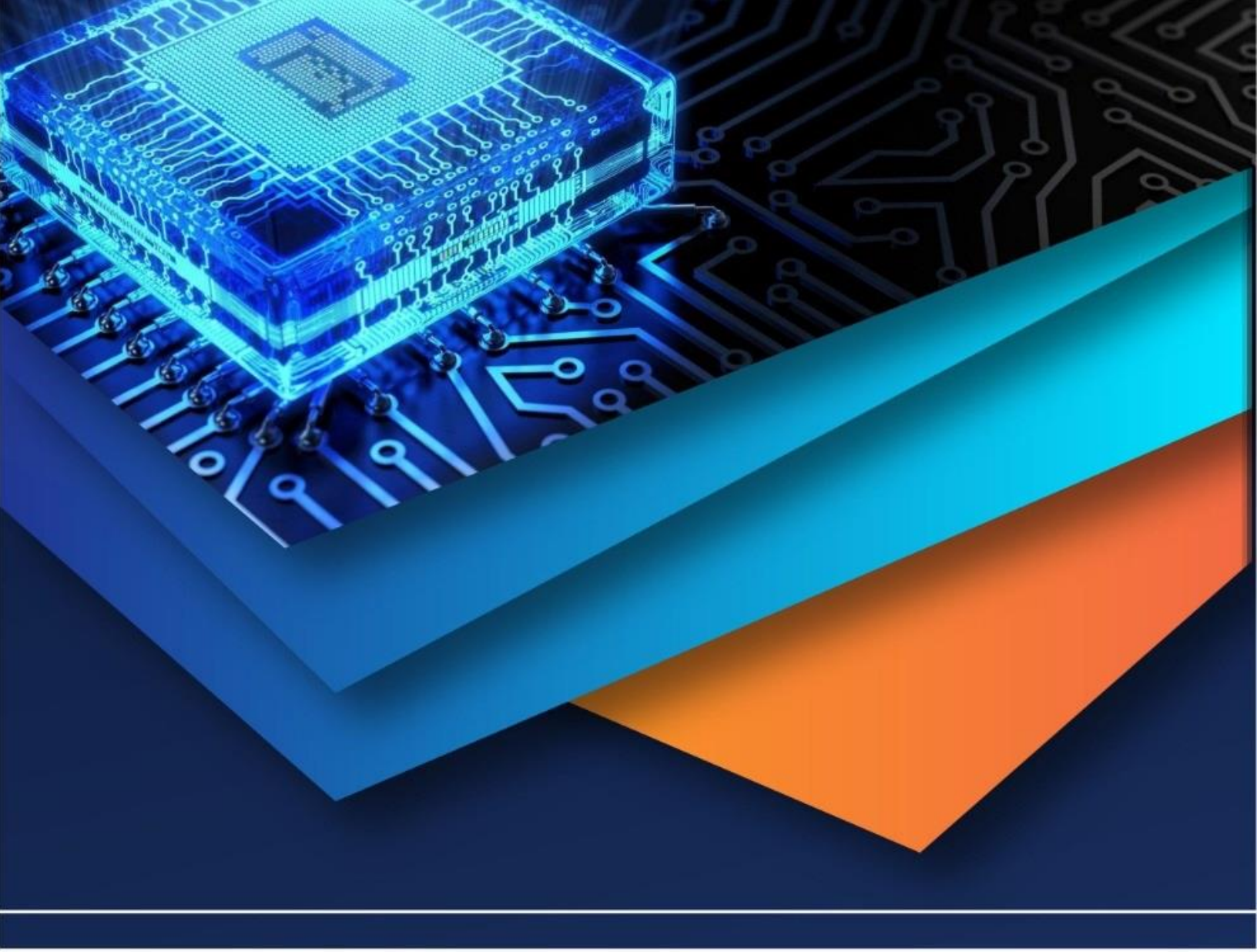
Using the dark web is a sensible think to improve your organization's security posture. Only if you take preventive security measures, including dark web monitoring, conducting regular penetration testing to find any vulnerabilities in your network and implementing regular security awareness training for all employees to learn your workforce about how to spot and report cyber threats

These hacks can cause setbacks to your organization. it's important to take such security measures to minimize the number of cyber-attacks. You can also secure your organization's data from hackers by using strong security measures.

The best thing about using the dark web is learning how your critical business information can be protected from hackers and cyber criminals.

REFERENCES

[1] Matías Porolli — Cybercrime black markets: Dark web services and their prices - 31 Jan 2019
[2] Falk Rehkopf — What you need to know about the Dark Web - 26 June 2018
[3] Chris Dickson and Kevin Birk – Data Flow in the Tor Network - 17 Jan 2016
[4] Photon Research Team – Dark Web Monitoring: The Good, The Bad, And The Ugly - 11 September 2019
[5] G DATA Guidebook – What actually is the Darknet? - 03 May 2019
[6] Craig Wilson – How does dark web help cyber security experts improve business security? - 11 FEB 2022



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY