INSE 6610 - Cybercrime Investigation
Underground Hacker Forums

Shivam Patel
Concordia University

Ekta Patel
Concordia University

***Abstract* - Internet forums have been increasing with the use of the internet worldwide. Millions of people use these forums to exchange information/knowledge. Underground hacker forums term used to point out forums used by hackers to chat, exchange knowledge, share malware. These forums are also used by hackers to sell credit cards, exploits, databases, etc. This study will describe information on past/current famous hacker forums on surface web as well as on tor network.**

Keywords - Underground hacker forums, darkweb, tor network, illegal.

1. INTRODUCTION

Internet is the best tool to share information all over the world. Especially when you are far away from your opposite party and you want to exchange data in terms of seconds. Forums are one of those services that enable people to communicate on certain particular threads. There exist a lot of forum sites that allow users to share, edit, delete their opinions but in a certain manner. The Internet can generally be divided into 3 parts. a) Surface Web, b) Deep Web and c) Dark Web

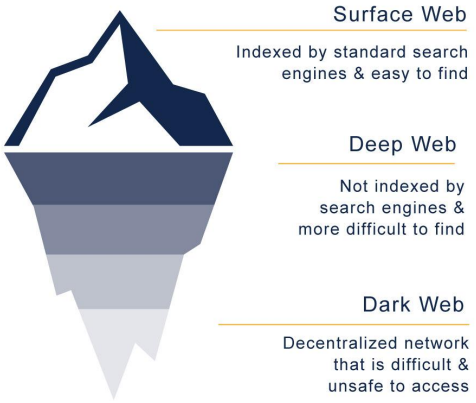

Fig. 1) Parts of the internet [1]

2. SURFACE WEB

Surface web is basically what normal users access the part of the internet. It is generally indexed by the search engines like google, yahoo, bing etc. All the surface websites are visible to people and they can interact with them in their daily life. Surface web is only 4% of the entire Internet. Surface web can be easily accessible by normal web browsers.

3. DEEP WEB

Deep web is generally considered as part of the web which is not indexed and crawled by search engines. This part of the web is not accessible by the general users. It generally consists of private data, medical records, research journals, private

forums, cloud storage, banking details, military information etc. Someone with special access control permissions can access these data who is incharge to maintaining/operating/viewing them. Deep web generally covers 90% of the whole internet means most of the data is protected by some kind of access control mechanism which is not meant to be accessible for the general public.

4. DARK WEB

Dark web consists of hidden websites that are generally accessible through a special protocol called Onion Routing. Using the TOR browser, we can access these websites and navigate around them. The dark web is known for the anonymity and privacy it provides to users. It generally covers up to 6% of the whole internet. Dark web websites use ".onion" top level domain names, which are not indexed by standard search engines. Dark web is generally known for illegal criminal activities such as drug markets, weapons sales, hacking services, stolen credit card marketplaces, database selling etc.

Underground hacker forums generally accessible on both, surface as well as dark web. These forums have been used by a lot of criminals, hackers to exchange information or services. In the past, IRC channels used to be very famous for hackers to chat with each other, share hacking knowledge, malware distribution etc. Which is then taken over by these underground forums. Nowadays discord servers, telegram groups and forums are main channels for hackers to communicate with each other. There are several underground forums that still exist on the surface web which are still used by people. Some of them recently seized by the FBI and other agencies apart from this their head admin arrested for different charges.

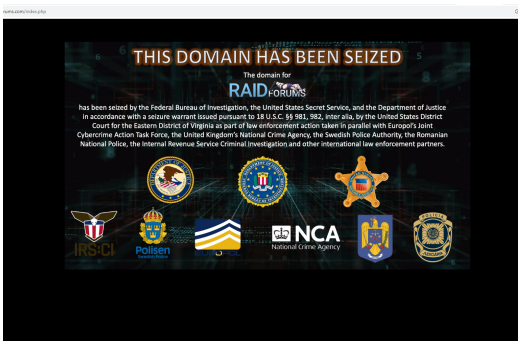

Fig. 2) FBI seized forum

5. FORUMS

a) Onniforums

Onniforum is one of the most famous forums. There are different topics on the forums. It is available on both surface as well as dark web. Their functionalities are very similar. Even they share the same database because users can register on a surface web account and use the same account to log in into the dark web version. Registration rules for account creation are very similar to other forums.

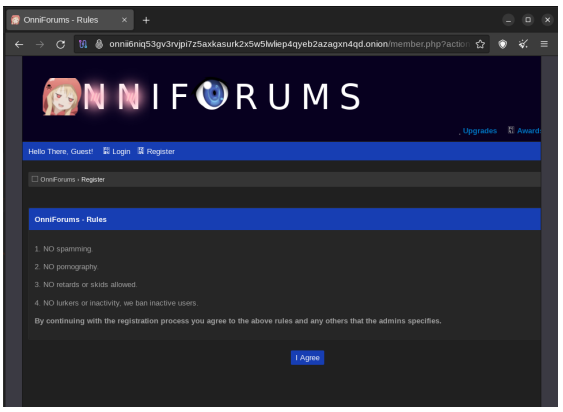

Fig. 3) Registration rules

Registration process only asks for username, password, image verification, referrer (optional) and security question. There is no email option so if the user forgets the password then there is no way for the user to recover the account unless they somehow are able to ping the admin of the forum and admin manually reset the password which is very rare. Again this process is the same for both versions and they reflect the changes on the user account.

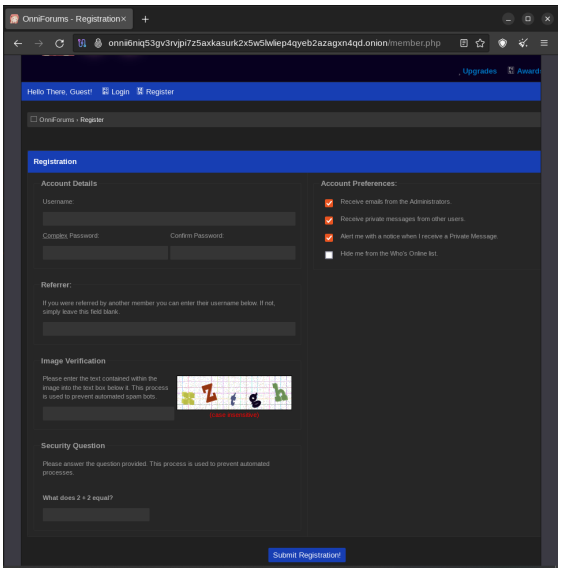

Fig. 4) Registration requirements

Login flow only required username and password. Once credentials are provided, it redirects users to the home page of the site. There is a shoutbox on the home page. It shows messages from random users and gives you a text box to chat there. There are various topics on the home page as well below the shoutbox.

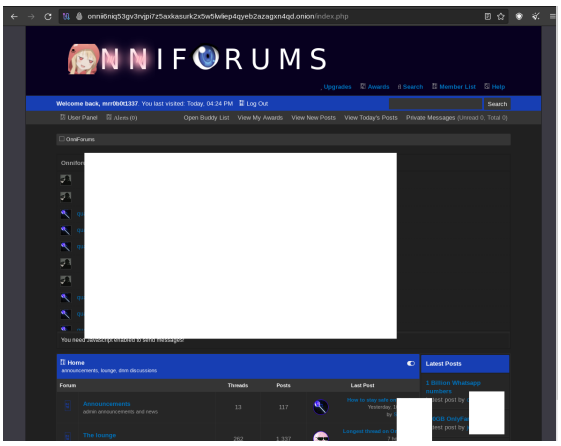

Fig. 5) Home Page

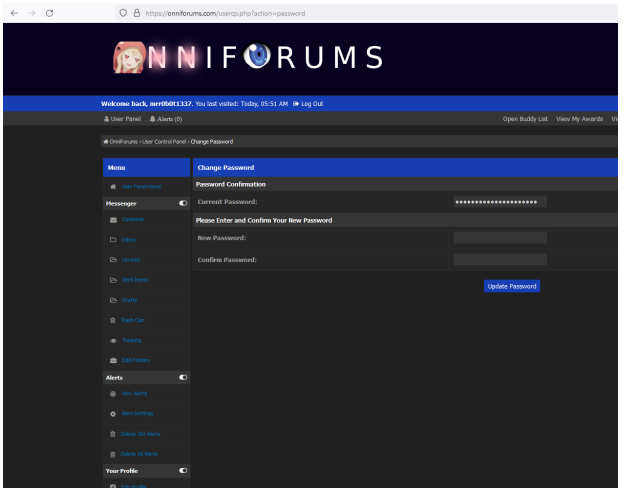

Fig. 6) Surface web Page

These all webpages are similar for the .com version as well as .onion version. If a user changes the password on a surface web forum then must use the same credentials to login on the dark web version. So all the changes take place on both versions if applied to any one of them.

This forum has a lot of categories of topics so interested one can choose any of them. They have main categories as hacking, market, leaks, development, carding, drugs

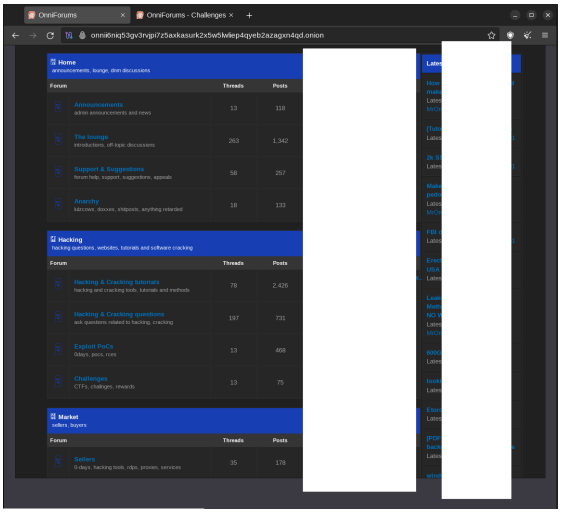

Fig. 7) Categories

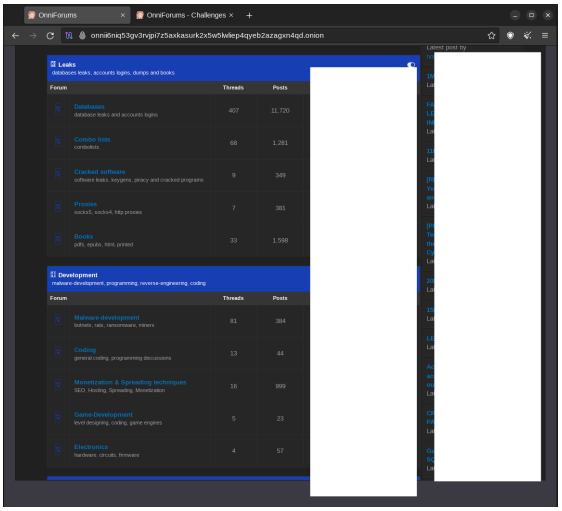

Fig. 8) Categories

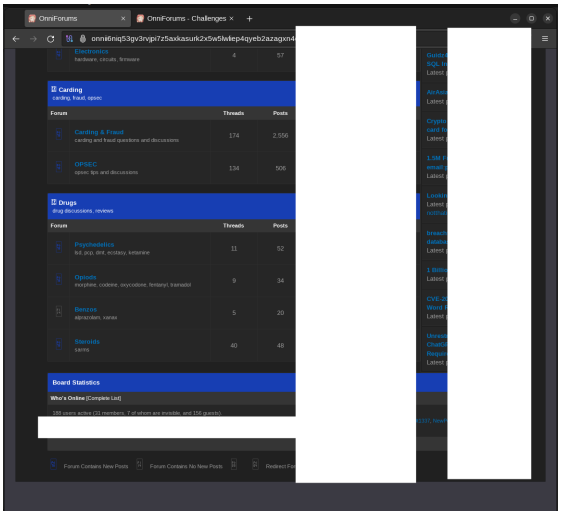

Fig. 9) Categories

This forum is use for credit card selling, selling zero day exploits, teach hacking, offer social media hacking services, DDoS services, Database leak or selling, distributing malwares, providing cracked softwares, proxies scripts, providing compromised ssh remote server, books, selling illegal substances, selling weapons, selling personal IDs etc.

Not all of the people visiting this website are doing any illegal activities. They just visit here to gain knowledge, chat on various topics, learn skills like web development and meet new people. Apart from this a lot of teenagers or adults learn hacking through discussions. There are so many threads talking about reverse engineering, web application hacking, binary exploitation, android hacking, iOS hacking etc. Active community of geeky people discuss various things over here.

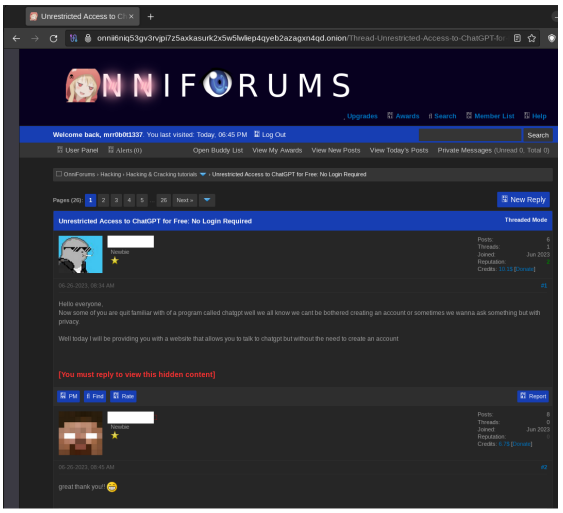

Fig. 10) Categories

One weird thing is that when users are looking for any information or data, they are kept hidden. Users have to compulsory

post the comment on that particular forum in order to see the information.

It seems hard to track ISP for the onniforum onion version but easier on the surface web. Using the whois services it is more convenient to find information.

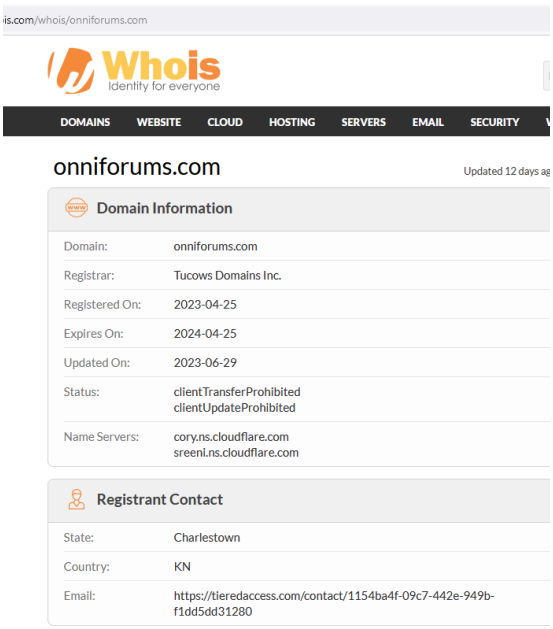

Fig. 11) Whois details

They registered a domain with Tucows domain inc. and it is valid till 25 April, 2024. Name servers belong to cloudflare so it might be possible that they are using cloudflare services somewhere in their infrastructure. Also the country of the registrant is Saint Kitts and Nevis.

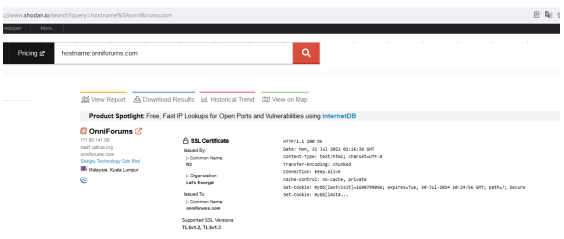

Fig. 12) Shodan details

To find their backend ip, I queried shodan search engine with a filter called "hostname" which returns the IP address of the host. The ip address returned by shodan is from Kuala Lumpur. Same IP address is shared by mail1[.]qithub[.]org.

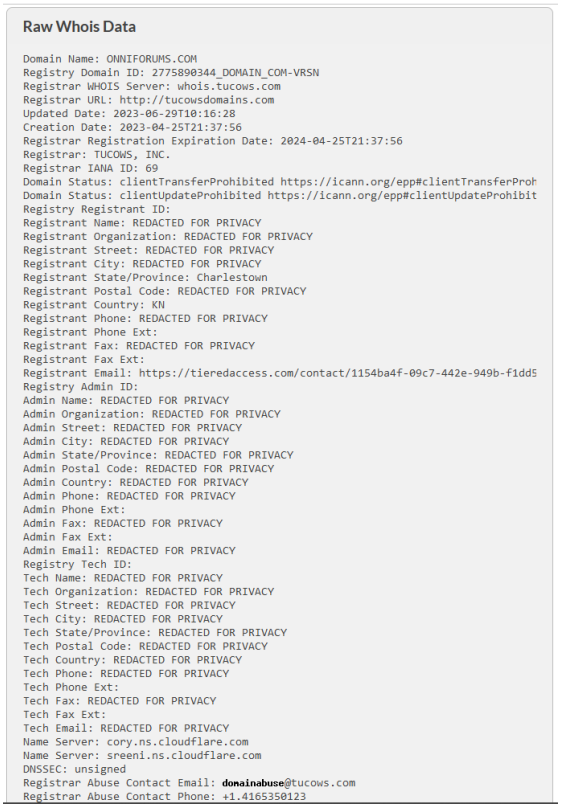

Fig. 13) Whois Raw details

The certificate for the domain is issued by the Google Trust Services LLC.

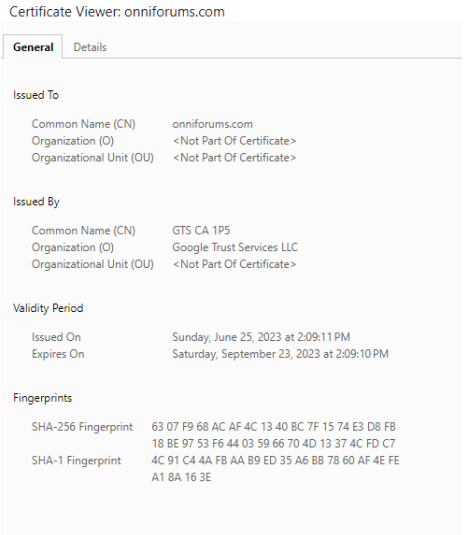

Fig. 14) Certificate

b) CryptBB

CryptBB is also one of the most famous underground hacking forum on the dark web. It is mostly similar to onniforums. The UI of most of these forums are pretty much very similar because the admin consists of one or very few people in the group. It is hard for a small group of people to make a website look nicer.

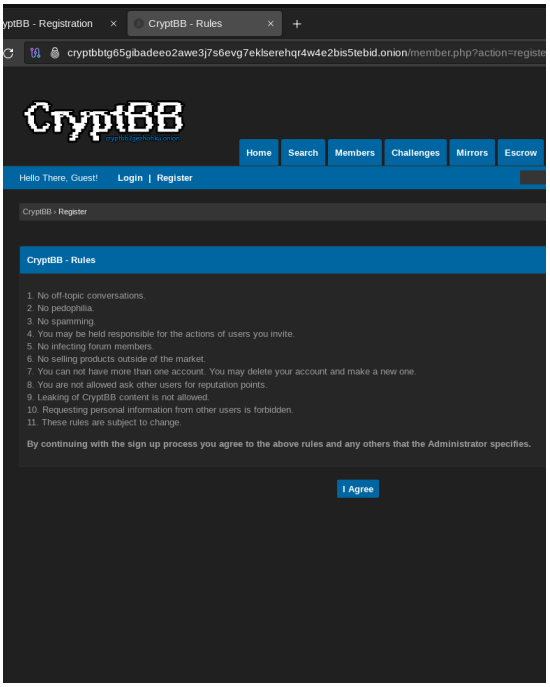

Fig. 15) Rules

The number of rules are more in comparison to onniforums. Also, the content of the website is prohibited to leak outside of the forum. Admin of the website can ban users if they miss conduct any steps that are not supposed to be done.

The user only needs to select username and password for registration. There is one image verification process similar to image captcha. These forums usually require username and password.

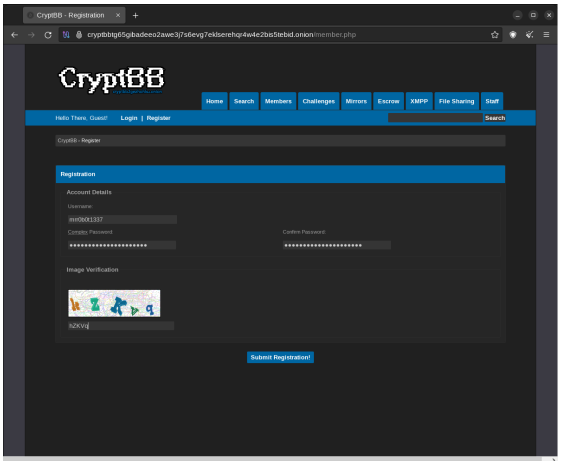

Fig. 16) Registration

Login flow just required username and password to login into account. This forum is very beginner friendly as they have separate forums for beginners who just started learning. Public section has different forums for newbies, programming, hacking, hardware, carding , training challenges, discussion and leaks. There is a marketplace for buying and selling different services. Buying service has no thread at the time of this survey but there are more sellers threads trying to sell credit cards, RAT, coding services, bank logs.

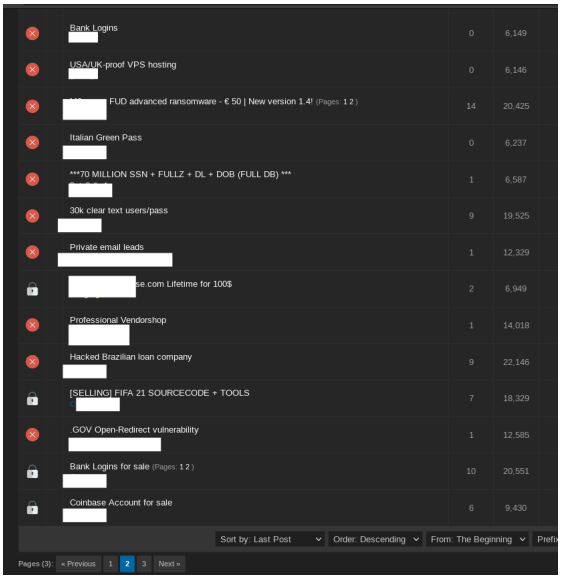

Fig. 17) Marketplace

It also allows you to send private messages to users and you will get a private default message from the admin when you create an account for the first time. Some pages are not accessible to normal users like members, mirrors, xmpp.

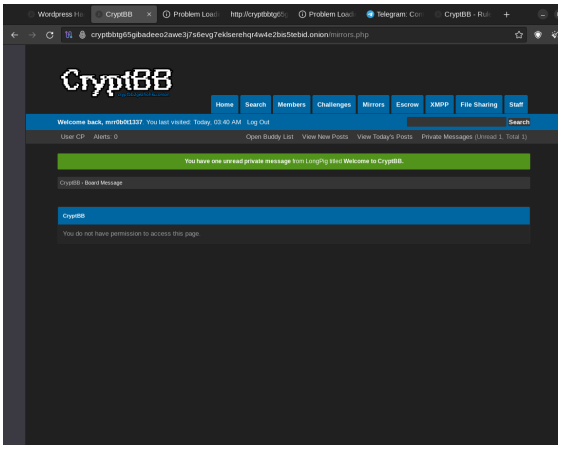

Fig. 18) No permission

There is also a challenges page which has hacking challenge and programming challenge. The hacking challenge is to find the password hash on that page and crack it to reveal the password. Then submit the password. For the programming challenge, they already provided the string so the task is to MD5 hash it and remove the last 16 characters of the hash and do this process 50 times and submit the final truncated hash. Also users can add other users to their buddy list which is similar to friends list.

c) Raidforums

Raidforum was one of the most popular forums on the surface web but it was seized by the law enforcement agencies in 2022. It promoted discussions on a range of hacking-related topics and was a prominent source of explicit content, hacking tools, and data breaches.

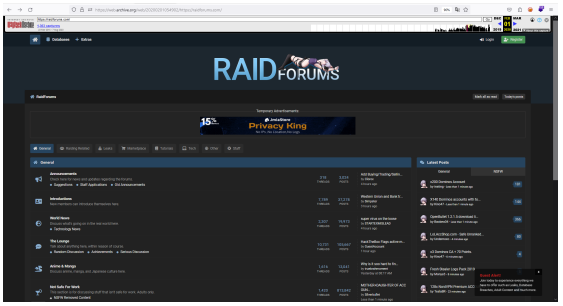

Fig. 19) Home[2]

This website was started by a 14 year old boy named Diogo (“omnipotent”).[13] In the beginning, the purpose behind this website was to provide a platform for the twitch raiders. In the past year, most of the data leaks were posted on the raidforums. People on this forum trying to trade stolen identities. It also used to share exploits, databases, credit cards, discussion related to hacking etc.

Diogo was on the radar of the FBI and he flew to usa. That’s where the FBI seized his device upon search warrant. They found a discord account with the name “Omnipotent” and a bunch of emails from the mail address of raidforum. FBI started gathering more evidence and took over the raidforum. This was where other users noticed that when they tried to enter the right credentials, the login page still stuck there and something was wrong. Some users were getting the idea that the forum was under the control of a suspicious party. That’s where a security researcher noticed that the Nameservers of raidforums afterwards pointed out to the address which was under control of the US Law Enforcement for hosting seized domains. They used the raid forum as honeypot to get credentials of other users.

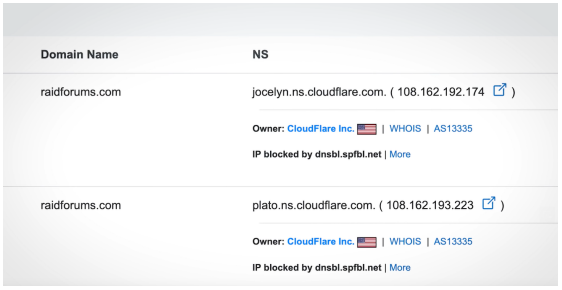

Fig. 20) Domains pointing out to other Nameservers

The FBI then announced the seized domain. They took help from other agencies to arrest Diogo in the UK.

d) Most common

Nowadays, hackers also use discord as their communication platform. There are a lot of discord servers that are carrying out the same threads in the form of channels. Database sharing on discord servers has become very often nowadays. Hackers also use these servers to communicate, learn, sell their resources, and share their plan to carry out different attack on the target.

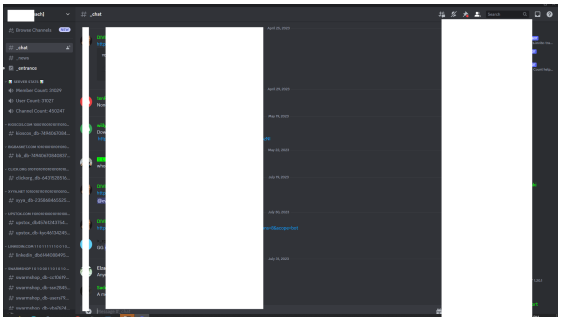

Fig. 21) Discord Server for Data breaches

Telegram is also one of the famous application nowadays to create a group and carry out the same activities as any forums do. Most hacktivists or criminals also use telegram channels to post their messages or let other people know about various things.

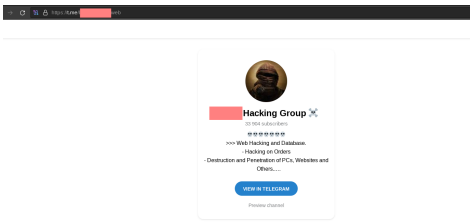

Fig. 22) Telegram group

6. CONCLUSION

These forums exist in a wide amount of range and it is not possible for law enforcement agencies to track them all as well as shut them down. Illegal activities such as selling databases, credit cards, personal identity, exploits are mostly seen in these kinds of forums. They don't have very great UI and most of them looks very similar to each other. Most people use these services to exchange their knowledge while staying anonymous on the internet. But some of them use these kinds of services for illegal purposes.

REFERENCE

1] IMAGE
https://mediasonar.com/wp-content/uploads/2021/02/Untangling-the-Web-Iceberg.jpg

2] Wayback machine
https://web.archive.org/web/20200201054902/https://raidforums.com/

3] Hacking Forums Raided By The Feds, Head Admin Arrested
https://www.youtube.com/watch?v=smUkjnYTSsw

4] Wikipedia
https://en.wikipedia.org/wiki/RaidForums

5] Surface Web vs. Deep Web vs. Dark Web: Differences Explained
https://blog.knowbe4.com/what-is-the-difference-between-the-surface-web-the-deep-web-and-the-dark-web

6] Onion routing explained
https://privacyhq.com/documentation/onion-routing-explained/

7] Top 5 Underground Hacker Forums That are Accessible via Your Web Browsers such as Google Chrome, Firefox, and Internet Explorer
https://socradar.io/top-5-underground-hacker-forums-that-are-accessible-via-your-web-browsers-such-as-google-chrome-firefox-and-internet-explorer/

8]Notorious hacking forum shuts down after administrator gets arrested
https://techcrunch.com/2023/03/21/notorious-hacking-forum-shuts-down-after-administrator-gets-arrested/

9]Dark Web Threat Profile: pompompurin
https://socradar.io/dark-web-threat-profile-pompompurin/

10] What is the Deep and Dark Web?
https://www.kaspersky.com/resource-center/threats/deep-web

11]Deep Web: Definition, Benefits, Safety, and Criticism
https://www.investopedia.com/terms/d/deep-web.asp

12]Surface Web, Deep Web, & Dark Web: What's the Difference?
https://macsources.com/surface-web-deep-web-dark-web-whats-the-difference/

13]RaidForums: The child hacker facing extradition to the US
https://www.euronews.com/next/2023/06/02/raidforums-the-child-hacker-facing-extradition-to-the-us