Study of Underground Hacker Forums

Pranshu Mainrai (40206628)

Collins Chukwu (40184336)

Aayush Mehrotra (40191642)

Ishan Chaudhari (40192935)

Hussein Al-Masaabi (40182554)

Sahaj Vinayak (40196687)

Shyamanuj Yadav (40218973)

*Abstract*—The cybersecurity problem is becoming more and more complicated due to the Internet's rapid development. Numerous underground forums or markets are currently available on both the surface and dark web, and they are crucial components of the ecosystem supporting cybercrime. To identify important hackers and gather reliable cyber threat intelligence, cybersecurity experts typically concentrate on hacker-centered research on cybercrime. Key hackers only make up a small portion of underground forum users, despite the enormous data volume of these communities. Therefore, it is necessary to identify the details of these forums and understand how they work. And find different ways to mitigate this problem arising from these underground forums.

*Keywords—deep web, cybersecurity, marketplace, dark web, social networks*

# Introduction

The Internet's depths extend well beyond the surface information many people may quickly access in their routine searches. The additional content is from the Deep Web, which has not yet been included in standard search engines like Google. Content that has been purposefully hidden can be found in the Dark Web's most remote regions or the Deep Web. The Dark Web can be utilized for noble causes and to hide illegal or otherwise immoral behavior. Officials and legislators are interested in how the Dark Web is being used for unlawful activities. Individuals can access the Dark Web using special software such as Tor (short for The Onion Router). By routing users' web traffic through several other users' computers, Tor uses a network of volunteer computers to ensure that the originating user cannot be identified from the traffic. Although accessing the Dark Web via these methods does not anonymize activities, some developers have devised solutions, such as Tor2web, that may allow users to access material without downloading and installing the Tor program. Once on the Dark Web, people frequently search for content using directories like the "Hidden Wiki," which lists websites according to a category, much like Wikipedia. People can use search engines to look for illegal goods like drugs, weapons, or counterfeit money. These engines might be general or more focused, looking over the Deep Web. People can communicate using the Dark Web via secure email, online chats, or Tor-hosted personal messaging. Although solutions like Tor strive to anonymize content and activity, researchers and security experts continuously create ways to identify or "deanonymize" certain concealed services or people. Tor and other anonymizing systems have been used for both legitimate and unlawful purposes, from safeguarding privacy to selling illicit items that were paid for with Bitcoin or other virtual currencies. They can be used to get around censorship, access content that has been restricted or protect the confidentiality of private discussions or business ideas. However, various nefarious actors, including terrorists, criminals, and state-sponsored spies, can also use cyberspace. The Dark Web can be a discussion, planning, and active place. It is unclear how much of the Dark Web is currently utilized to support a specific black market. It is much more difficult to determine how much traffic is going to any site because of the anonymity provided by services like Tor. Just as criminals can rely upon the anonymity of the Dark Web, so can the law enforcement, military, and intelligence communities. For instance, they might employ it for anonymous tip lines, online sting operations, and monitoring. On the Dark Web, anonymity can protect authorities from being tracked down and hacked. Additionally, it can be used to carry out a covert or clandestine computer network operation, such as the denial-of-service assault, bringing down a website, or intercepting communications. Officials are constantly developing new methods to deanonymize Dark Web activity and cyber criminals.

# Background and related work

Web forums are among the first and most fundamental forms of Internet communication, and the idea of a forum dates back even longer. Web forums first appeared in the early 1970s. The emergence of the carding forum Carder Planet in the early years of the new century solidified a paradigm that was imitated by all subsequent forums run by cyber criminals. Cybercriminals still utilize forums to get guidance and talk about the newest methods and advances, much as they did in the past.

Communication and trade systems have emerged, offering better efficiency, simplicity, and security compared to the cumbersome thread-and-post approach employed by forums. There are centralized systems like blockchain DNS (Domain Name System), i2P, and BitTorrent, as well as messaging services and encrypted applications like Telegram, Wickr, and Discord. Marketplaces and AVCs are two examples of automatic trading platforms that have established themselves in the industry.

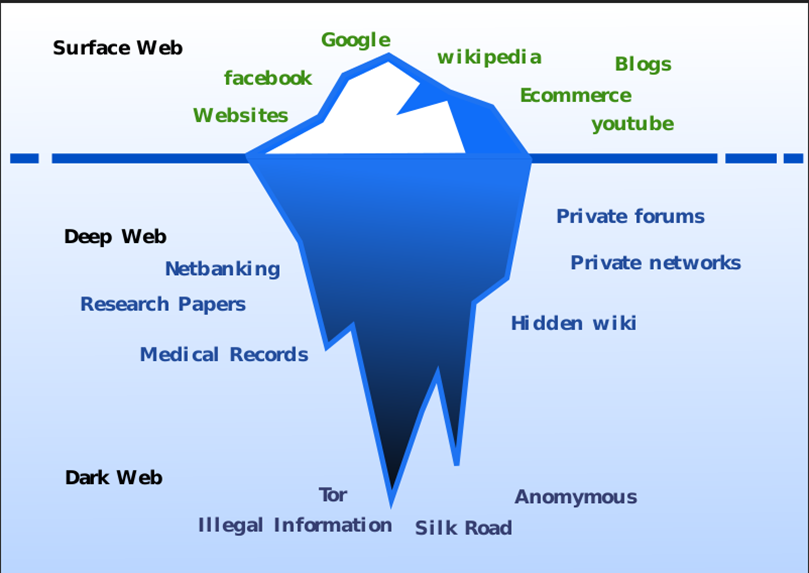
Supply and demand are the driving forces behind underground market businesses, just like in standard ones. An instrument or piece of knowledge is worth more the more esoteric it is. In contrast, when a market is oversaturated with products (such as credit cards), the price per unit drops.

In contrast to traditional enterprises, these businesses run more like a market-driven fair economy of buyers and sellers, each of them serves as an independent contractor and adds value to the community. These independent contractors are free to choose their hours and frequently have a second job to support their activities.

Operating principles and forum regulations are present in hacking marketplaces. A hacker's code of ethics is followed by white hats. The criminal, however, has always behaved unethically.

# Darknet and clearnet

All the websites and data available on the internet can be categorized into 3 parts **Surface Web**, **Deep Web,** and **Dark Web**.



**Clearnet** is a term that typically refers to the publicly accessible Internet. Clearnet is the synonym for the surface web. The World Wide Web is one of the most popular distributed services on the Internet, and the surface web is composed of web pages and databases that are indexed by traditional search engines. Clearnet is just 4-5% of the whole internet and almost 90% of the people access the surface web only for almost all their needs. Typically accessed websites on Clearnet are Google, Facebook, Wikipedia, YouTube, Blogs, and e-Commerce websites. We can access them using any general web browser like Mozilla Firefox, Google Chrome, and Safari.

Now, coming to the under-the-surface web, the terms we commonly hear are “deep web” and “dark web” they are sometimes used interchangeably, but they are not the same. Both deep web and dark web together constitute about 95-96% of the total internet websites and webpages. **Deep Web** is an umbrella term used to access data that is unindexed and censored by the standard web search engines. It can still be publicly accessible and can be located and accessed by a direct [URL](https://en.wikipedia.org/wiki/URL) or [IP address](https://en.wikipedia.org/wiki/IP_address), but may require a password or other security access to get past public pages. It includes web portals to databases that require text searches and interactive websites that require more user input than simply clicking hyperlinks. The content of the deep web is hidden behind login forms and includes uses such as webmail, [online banking](https://en.wikipedia.org/wiki/Online_banking), restricted access to social media pages and profiles, some [web forums](https://en.wikipedia.org/wiki/Web_forums) and code language that require registration for viewing content, and [paywalled](https://en.wikipedia.org/wiki/Paywall) services such as [video on demand](https://en.wikipedia.org/wiki/Video_on_demand) and some online magazines and newspapers. It offers the opportunity to bypass local restrictions and access TV or movie services that may not be available in their local areas. Others go somewhat deeper to download pirated music or steal movies that aren't yet in the cinema.

**Dark Web** is a hidden part of the world wide web that can only be accessed using a special browser known as [Tor](https://vpnoverview.com/privacy/anonymous-browsing/tor/). Dark web pages don’t appear when you look for them in a search engine, so you need to know the exact address of the website you want to visit. Specific browsers, such as Tor Browser, are required to reach the dark web. It consists mostly of illegal products or content that could be harmful to organizations or the public. Some examples include stolen credit card numbers, fake IDs, drugs, illegal weapons, stolen/ fake merchandise, child pornography, and cannibalism-related stuff and you can hire Hitman here as well. To access the dark web, a user needs to download darknet software, the most popular being Tor. All the dark web websites have an extension ‘. onion’ which normal browsers can not only browsers as Tor can. They are either invite-only websites or are encrypted as websites to remain hidden deep in the world of the internet. Tor, which stands for “the onion routing project,” was developed by the U.S. Navy for the government in the mid-1990s. It was open-sourced in 2004, and that’s when it went public. Today, Tor is the dark web browser that most people use to surf the internet anonymously. To do this, Tor hides a user’s IP address (or the unique address that identifies an internet-connected device or network) by bouncing their search request to multiple different locations. These bounces also referred to as relays, make it much harder for people to find users on the dark web. Today, it is funded by many big organizations like DARPA, Mozilla, US Department of Bureau of Democracy, Human Rights and Labor, Google Summer of Code, Ford Foundation, and many more.

**Hacker goods for sale**

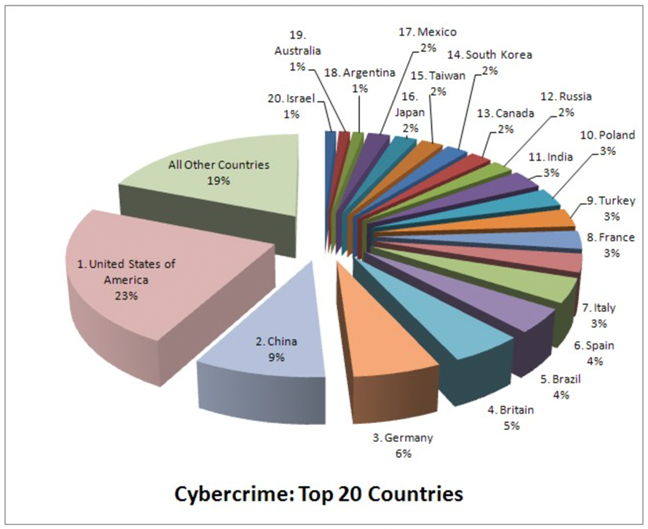
The tools used by hackers are custom made and some of them are the ones that were created for research purposes but looking at their potentially harmful effects than the benefits they were never released to the public but are somehow common in the underground world and are used by miscreants to do notorious stuff.

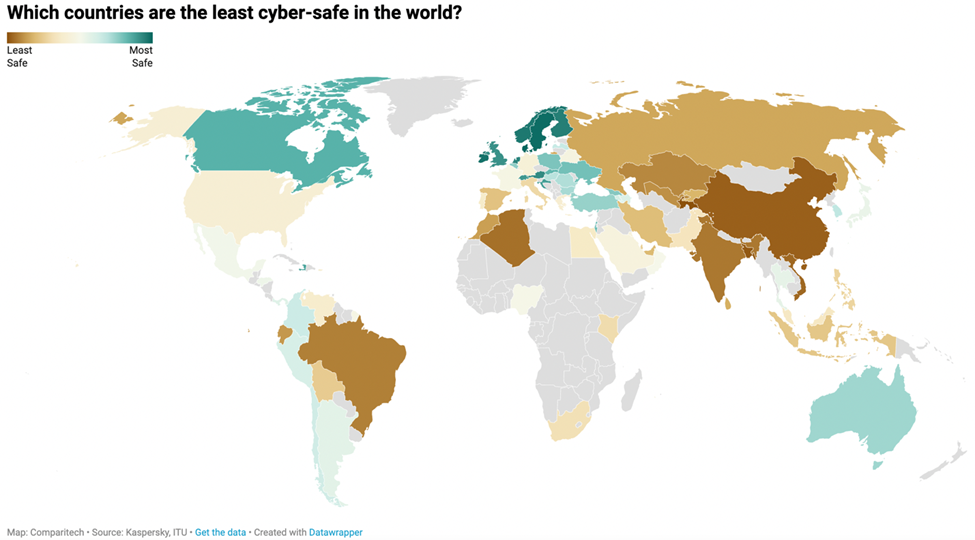
“S in IoT stands for security”. When you look deeper into an IOT device or any embedded device for that matter, what do you see? You see windows of opportunities. Opportunities to modify it. To edit it. To exploit it. To hack it. IoT devices are full of vulnerabilities.

These are cheap and easily accessible hacking tools which are available. So far, Kali Linux has been the best and most widely Operating System, filled with an awesome collection of hacking tools which can be used for Web Application penetration testing, network security testing, and WiFi attacks; best of its kind. It is the most famous and most useful Operating System used by security enthusiasts, and hackers – both white hat and black hat, as well as hobbyists who like to tinker around with Linux OS.

There are many hardware tools that can be used with this software and a few of them are Ubertooth One: for Bluetooth hacking, and Alpha USB Wi-Fi adapter: for illegal wireless activities. Raspberry Pi: is a minicomputer on which you can install a hacking OS. Plastic Card Clone: for cloning debit/credit card information, RFID reader: for reading all the information from RFID-equipped devices in the vicinity of this reader, and many more other things which are a bane to society rather than a boon.

Below is a pie chart indicating the most cybercrime-affected countries





# Data Leaks and where do they end up?​

## Graphical user interface, text, application, email Description automatically generated

We have heard about major corporations getting hacked and having their data stolen. So, where does it end up?

The data ends up on such forums. One such forum is called RelateList. Below are some screenshots of the leaked data banks we found while researching for this. The website claims to be legitimate by having “connections” but contains documents and data that are privacy sensitive. Similarly, there are so many more hacker forums that do not bother to look legitimate and directly post data leaks for purchase. Unfortunately, we didn't find any that were still online and running. ​ Graphical user interface, application

Description automatically generated

# ​ Ecommerce and Selling on hacker forums​

Some forums are helpful, whereas many are blatant scams. Most of the forums we came across have urged us to purchase “leaked” credit cards containing huge monetary amounts for as low as 50$. There’s no actual way of knowing if the websites are a scam unless we pay, but nobody is going to offer 3000$ worth of credit cards for the price of 20$ (intuition).

A picture containing text, monitor

Description automatically generated

Fig. showing the different financial accounts for sale on a popular hacking website

However, there are some websites where you can approach other hackers to hack for you. Similar to hiring a hitman. Many of these websites are hosted in Russia/ Ukraine and some are currently inaccessible due to the war tensions in the area. A lot of the websites also force you to create an account to access but due to the websites being available in the Russian language only, it was difficult to navigate around for the research.

Timeline

Description automatically generated with low confidence

Fig. showing a seized website by the security agencies

We also came across forums that have been seized for misuse or violation of country laws & policies.

## Creating an account on Hacking Forums​

Text

Description automatically generated

Fig. showing dark web links

* For creating an account, we here will take the example of blackhost. It is a darknet website and can be only accessed via the tor browser.​
* After making sure, we are connected to the tor network. We can find this website by accessing the hidden Wikipedia or the uncensored hidden Wikipedia. ​
* The hidden Wikipedia allows us to access current active links easily for most websites such as WikiLeaks, filesharing websites, darknet social media and email providers, and some extremely illegal websites as well. There are tor search engines such as haystack, torch, or notevil. But these search engines show too many spam links along with the original link. Which could be difficult for a newbie to distinguish.​
* Hidden Wikipedia usually has trusted links. We can also search for such forums on the hidden answers forums, where we can ask a query and get anonymous answers. ​

## After account creation

Text

Description automatically generated

Fig. showing a popular dark website BlackHost

* Once you have navigated to the blackhost website, you will be greeted with the following screen. ​
* Here, we are allowed to access limited resources, and similarly to Clearnet websites, we would be required to log in for accessing the full functionality of the website such as chatting with other hackers, uploading files, and interesting games that improve our hacking skills, webmail, and other such services.​
* To create/login into our account, we simply click the user button, and we will be redirected to a new page.Graphical user interface

  Description automatically generated

Fig. showing the login of BlackHost website

* Once we have successfully logged in, we can navigate around the website normally and have access to the entire website including chat features and mail services. Through these chat services, you can get in touch with other hackers willing to help us out with any information we need. Such forums also allow us to hire hackers.​

# What internet service providers do underground hackers use​

Table

Description automatically generated

The underground hackers leverage the normal internet broadband infrastructure available to legitimate users. While the cybercriminals stay anonymous on the internet and operate strictly within their defined ecosystem, the other random legitimate users are visibly on the internet platforms for legal profits. Access to the forums is strictly on invitation and all activities are undertaken using anonymizing protocols and/or Clearnet. To reach a wide range of audiences, the sale of services is done through underground marketplaces that are usually shrouded in secrecy. The underground hackers exploit vulnerabilities in existing software platforms to hack into suspecting user accounts, illegally mine data, and provide the following common services. Money laundering, DDos, Botnet, Exploit kit, 0day, Crypter, Doxing, Hire a hacker, Spam, Malware, etc. Rented botnets are used to run spam or for DDoS campaigns, users pay negotiated prices depending on the desired number of attacks, targets, and duration. Deep Web has been defined as a “hidden reality” where various illegalities such as goods, products, and services thrive. The black-markets segments of the Deep Web provide sellers with protections to trade their wares without being caught by the eagle eye of law enforcement agencies. It’s a haven for fake identities, drugs, weapons, counterfeit, stolen merchandise, credit cards, access to bank accounts, trafficking in persons, organs, hacking services, etc.​

## Hot Topics in Deep Web​

There are many hot topics trending on the Deep Web which include but are not limited to the following. ​

1. Credit card numbers mining & sales. ​

2. Bank accounts and routing numbers. ​

3. Voter registration information ​

4. Employee Login credentials & other personally identifiable information. ​

5. Drug database ​

6. Public records database. ​

7. Crime Database ​

8. Toxic chemicals database ​

9. Housing database. ​

10. Child pornography database​

## Principal players of the hacking on the deep web

The key players in the deep web underground marauders are as follows: ​

1. TOR (Majestic Garden) ​

2. MRNiceGuy (TOR, a clone of the original​

3. TOR (Outlaw) ​

4. Agora (TOR) ​

5. TheRealDeal (TOR) ​

6. SilkRoadReloaded (12P) ​

7. DreamMarket (TOR)​

In the black-market categories, the following are existing. ​

8. Lampeduza.​

9. Rescator

Text

Description automatically generated

Fig.- Showing different prices on a dark web AccMarket

## Mitigating Buyers Risk.

Timeline

Description automatically generated with low confidence

Fig. showing the relation between the key players of the dark web

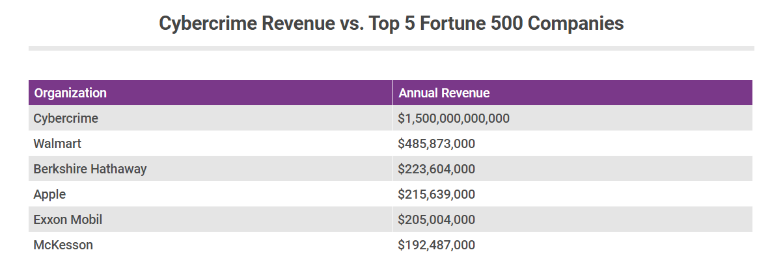
To mitigate product/services buyers’ risk in the deep web jungle, the black market is hosted in the Darknet for buyers' and traders’ navigation. This platform shields their activities from law enforcement agents who go after them. However, users are still prone to falling prey to the law enforcement honeypot. Government agencies are also able to intercept physical truckloads of real and illegal products like drugs or weapons​.

# Dark-web marketplace transactions​

Since Silk Road, the first successful dark web marketplace, emerged in February 2011, online illicit marketplaces known as crypto markets have drawn significant attention from the media, government authorities, law enforcement organizations, and researchers. Although they share many characteristics with genuine online marketplaces like eBay, these new online marketplaces put a strong emphasis on anonymity and security to reduce the risk of identification. The development of crypto markets was facilitated by two online anonymizing technologies. Bitcoin is the first (Bitcoin).

Blockchain-based digital money called Bitcoin is completely decentralized. Bitcoin payments are anonymous until the Bitcoin addresses and transactions can be linked to specific people, even though all transaction data are accessible to the public. The second technology is the Tor network, which builds a barrier between users and the websites they access by routing messages through several relays. This makes it challenging to pinpoint the location of a website user. Administrators of dark websites can escape law enforcement by hiding the location of their website servers. Numerous crypto markets have been established since Silk Road was shut down and its operators were detained in October 2013 because of increased scrutiny from the relevant authorities.

Several illegal online marketplaces have been taken down by law enforcement agencies in a few success stories. However, there are still hundreds of thousands of active dark markets.

  
Sources: [Into the Web of Profit Report](https://www.scribd.com/document/377159562/Into-the-Web-of-Profit-Bromium-Final-Report) and [Fortune 500](http://fortune.com/fortune500/)

Cybercrime is a very massive business that is rapidly expanding and involves more than simply "hackers in hoodies." As more of our regular activities move online, so too does crime, where the rewards for fraudsters are frequently bigger and the chances of being detected are typically smaller.

# Services provided by hackers and their prices​

* The average cost for a DDoS attack is $33.​
* Social media account hacking: In this attack, the hacker gains access to the passwords of the victim’s social media accounts. They give the passwords to the person who buys this service. This service costs around $295 per platform/account. The cost might vary with different platforms.​
* Email Hacking: In this type of attack, the hacker steals the password of the victim to gain access to the email. They either give it to the person who buys this or they themselves break in and access the data. The price for this attack averages $309.​
* Computer and phone hacking: Here, the attacker break into the system to deploy malware or steal data from the targeted computer or phone. The cost of this attack is $441. The cost remains the same for all the OS.​
* Website Hacking: This attack consists of gaining access to the admin panel or gaining access to the database of the website. This attack costs $507.​
* Attacks on School servers: In this attack, the grades of students are altered. This attack can be conducted in schools and universities. This attack is very common amongst students. Students pay up to $676 for this attack.​
* Personal Attacks: A personal attack can include public defamation, financial theft, and legal trouble. Most hackers gain access to the computer of the victim and try to depict the victim as a buyer of child pornography. This attack costs around $708.
* Controlling device remotely: In this attack, the hacker gains access to a computer or a mobile device and controls it remotely. This attack costs around $1000.
* Package deals: There are many package deals available on hacking websites. One such example is, breaking into someone’s phone and computer and finding the information which is required by the buyer. This attack costs around $2320.
* All the prices on the website are given in bitcoins.
* Hackers only accept the job when they think that they can pull it off.
* The payment is to be made upfront as all the hackers demand money before they start working.
* Some hackers offer a refund if the attack isn’t successful.
* Sometimes, hacking prices vary on the ranking and experience of hackers on the websites and forums.
* Sometimes, law enforcement uses these websites as honeypots. There is always a risk that a buyer falls victim to the honeypot websites and gets tracked by law enforcement.

Some websites through which we can hire a hacker are:

* RENT - A – HACKER
* Hacker for Hire
* The hell hacking forum
* The realdeal Marketplace

Graphical user interface, text, application, chat or text message, Teams

Description automatically generated

Fig. shows a chat between a hacker and a person selling Twitter account.

VIII) 1. Linguistic Characteristics

1.1 The CrimeBB Corpus

We function with sections of CrimeBB, a gathering of posts collected from various English and Russian-language forums that use the CrimeBot software outlined in Pastrana et al. (2018b) [1]. The HackForums is the world's biggest forum in CrimeBB; the earliest known HackForums posts were created over a decade ago, and the site has long been classified as the top hacking forum by Alexa.com [2]. Several high-level incidents involving denial-of-service threats and banking spyware have been linked to HackForums. In this paper, we examine CrimeBB subsets from a variety of HackForums bulletin boards, which include Beginner and Intermediate Hacking, High Price Sellers, and Remote Server Administration Tools [3]. These have been selected as a random sample of forum board types. We extracted some posts and analyzed them as defined below before training machine learning algorithms to automate the annotation procedure.

1.2 Annotation Process

To begin to understand our records and the difficulties they contained, we chose a sample of HackForums posts and analyzed each one for important variables. We chose a few posts from each of the following bulletin boards: Beginners' Hacking, High Price Sellers, and randomly selected boards ('combined boards') [1]. The classification process involves random selection from the history of the selected bulletin boards, filtering for comment sections with fewer than five posts, and repeating the process until the needed number of posts is reached. The posts were then annotated for three factors: post category, author purpose, and intended recipient [3]. These variables reflect our curiosity about what they say and to whom. The post type specifies the general purpose of the post and can be any of seven labels, as illustrated in Table 1 with descriptions. Products and services can be represented by diametrically opposed offerX and requestX; exchange posts occur when a user suggests trading an item and/or service for cash or another item and/or service in kind.

Tutorials are examples of information-based posts that include a relation or assist in revealing how to complete a specific task and are published for people to follow. Assistance, guidance, or information request is frequently the first post in a thread discussion. A comment is any informative response, whether it is the first post in a thread or a response to everyone else's post(s). Finally, a social post was made in which a user suggests additional interaction, possibly through another type of media, such as interconnected gaming.

Author Intent is concerned with the poster's effect and what they appear to have aimed at by the precise wording of their comments (Table 2). We suggest eight author motivation labels3, which include positive, negative, and neutral labels, which are a standard trio of labels in sentiment classification—the NLP field most close to resembling this task (e.g., Pang et al. 2002) [2].

Other author motivation labels include arbitrate, which is used when a user suggests that an earlier post doesn't relate to the existing message board or forum for whatever reason; when a user indicates that a service or product is legitimate and efficient (vouch), or when they want to thank some other users for their assistance or services (gratitude). It is important to note that these are both subcategories of positive intent, albeit more specific and serving operations essential to the presence of social relations in a web hacking forum [2]. There is also private messaging, which occurs when a user tries to transfer a conversation to another channel, including Skype or Facebook messenger, and aggressive behavior, which includes offensive language and an aggressive stance by one user toward others. Again, we also have a sub-type of an overriding label—in this situation, 'negative'—because we are concerned with the growth of antagonism in forum interaction [3]. In the absence of an obvious personal addressee, we switched back to a basic group label such as 'thread' (people involved in the discussion thus far) or 'bulletin board' (all users who visit the bulletin board where the thread is published).

2. Thematic analysis

Numerous themes emerged from the analysis, which is summarized below.

2.1 Learning new skills: A common theme across all sites was a desire to learn new programming and hacking skills. As a portion of this, there was a belief that attackers were frequently self-taught, but there was also recognition that formal education could be beneficial [3].

“It is about finding someone or a group of people you can trust enough to bounce ideas off and learn new skills. A lot of what is referred to as hacking can be learned right from Google”

While there appeared to be some respect for individuals trying to learn hacking on their own, it was also clear that there were higher chances for them to do so correctly, with some forum users showing low tolerance for newcomers who were considered to have made irrelevant comments or asked silly questions.

2.2 Legality: The legality of various actions was commonly discussed in conversations across all sites. A common scenario might be a user posting an inquiry on how to engage in an unlawful activity (such as gaining access to a social media account). While some practical advice may be given in reply to these questions, most comments will point out to the user that what they are requesting is illegal, sometimes even more critical that the users seem to have a skewed view of what hacking is [2].

“ahh my friend, you misunderstand the term "hacking," hacking does not say illegal infiltration of the DOD or anything like that, hacking is much more than that, it's making the most of what you have and making it work for you"

Users frequently disclosed that they had previously engaged in illegal activity and had received some form of a notification message from the specific target group provider declaring that they had been discovered. The comments to such posts ranged widely, from those advising that further activity would be unlikely for relatively minor violations (often framed sarcastically) to those instructing the user to take precautionary steps.

2.3 Risk: what levels of risk are acceptable? There was also debate about how to reduce these risks. These responses were commonly related to the theme of legality, with a financial analysis occurring in which the level of risk was mentioned in anticipation of possible legal repercussions if the participant was caught [3].

“Can anyone confirm is this is too risky now? I think I might take a break from it now”

2.4 Honesty: Users were frequently questioned about the truthfulness of their IDs and posted content. Users were queried about comments stating that they had been detained for an activity or that law enforcement had affected an online resource in use by hackers. Those who made the challenge provided several explanations for why the user seemed to be conveying a false story. In the case of posts about cybercrime as a service, it included recommendations that any such comments were an effort to drive business to the initial poster.

"Are you able to ban @\*\*\*\*?" He is telling lies and scaring everyone to gain more clients"

This pattern was related to risk and legality. In some cases, a user's honesty was called into question because a story they told was deemed unrealistic because the user lacked the skill that they claimed to have. This is related to the attention to the knowledge theme [3].

2.5 Knowledge: It was clear that knowledge plays a significant role in the identities of both organizations and users. Knowledge seemed to be the most important element in how people placed themselves in the hacking community. People characterize themselves based on their hacking knowledge, with a disdain for those who depend on software obtained online that does much of the unauthorized access for them (recognized as a script skid, skiddie, or kiddie) [2].

"The knowledge could be biased or simply incorrect; not to bash everyone who teaches hacking, but basically put, a very large number of individuals here don't know the first thing about hacking."

But besides this, it did appear that participants who proved a level of self-awareness about the boundaries of their knowledge got a less angry response, as well as an acknowledgment that the use of web hacking tools was an incredibly prevalent main gateway for those joining hacking.

IX) Security Measures for Protecting Against Cyber Threats

Different cyber security methods should be used by businesses to protect their client data, financial flow, and corporate data online. These steps should be taken to reduce hazards from a variety of sources, such as:

• online threats like spyware or malware

• User-generated flaws, such as readily cracked passwords or lost data

• inherent weaknesses and defects in systems or software

• interfere with system or software functions

Essential steps for cyber security

The following procedures and technologies are simple to implement and, when used together, will provide you with a fundamental level of security against the most prevalent IT dangers.

1. Adopt an employ-centric approach

Your strongest security shield or your worst security danger can both be people. The employees themselves are a crucial perimeter in people-centric security. Employers grant staff the freedom to use gadgets, handle information, and take security measures by:

• confiding in them

• putting them in charge of protecting the corporate data they utilize

However, you must make sure that every employee adheres to the cybersecurity best practices outlined in your security policy.

It's critical to comprehend both the threats that your employees could pose and how important they are to your cybersecurity.

The two most important factors to consider while attempting to defend your cyber environment are training and personnel monitoring.

1. Control system and data access

Ensure that people can only access data and services for which they have been given permission. You can, for instance:

• manage physical access to buildings and computer networks

• deny unauthorized user’s access

• Use application controls to restrict access to information or services

• limit what can be saved to storage devices and copied from the system.

• restrict the sending and receiving of specific email attachment types

Most of this may be accomplished with the aid of modern operating systems and network software, but you will need to manage user registration and user authentication processes, such as passwords. Read NCSC's introduction to identity and access management controls for further details.

3. Principle of Least Privilege

Avoid allowing too many people to access your data.

When new employees are given full access by default, they can access private information even if they don't need to. Such a strategy ups the danger of insider threats and gives hackers access to private information the moment one employee's account is compromised.

The use of the least privilege principle is a far better approach (POLP). In other words, grant the fewest privileges feasible to each new account and raise privilege levels as needed. And any corresponding privileges ought to be quickly revoked once access to private information is no longer required.

The zero-trust security model, which likewise aims to lower the risk of insider attacks by drastically reducing unnecessary trust, shares similarities with the notion of least privilege. According to zero trust, only those people and devices should be given access who have already been confirmed and authenticated by the system.

In conclusion, you can combine or switch between these three strategies to guarantee that you always grant privileged access to the appropriate users inside your organization.

1. Create hierarchical policies for security

A written policy, first and foremost, acts as a formal manual for all cybersecurity measures implemented in your firm. It gives you a mechanism to impose regulations that secure business data and enables your security specialists, employees, and managers to communicate effectively.

However, because every department's workflow is different, unnecessary cybersecurity techniques and measures might easily disrupt it.

Second, even while a centralized security policy can be useful as a general set of rules for the entire business, it shouldn't apply to every procedure in every division. Give your departments the freedom to develop their own security policies based on the main policy.

1. Put multi-factor authentication to use

For sophisticated security solutions, multi-factor authentication (MFA) is a requirement. MFA adds an additional degree of protection, making it very impossible for hostile actors to log in pretending to be you. This helps you protect critical data. A hostile actor would still require your second and maybe third "factor" of verification, such as a security token, your smartphone, your fingerprint, or your voice, even if they already had your password.

MFA is a basic implementation, but it nevertheless counts as one of the top cybersecurity measures. Because of its effectiveness, tech behemoths like Twitter and Google encourage their users to adopt it. A user account is more than 99.9% secured from hacking attempts when utilizing multi-factor authentication, according to one of the Microsoft security managers.

6. Backup Data which is Sensitive

7. Regular Audits for Cybersecurity

8. Simplification of security Infrastructure

X) Conclusion

One of the main foundations supporting the development of the underground economy is underground forums. These forums are appealing sites for young, unskilled people to learn about hacking because of the sense of anonymity they offer and the simplicity of access to attack tools and services. It is possible to think about early intervention strategies to steer these low-level hackers away from illegal activity by analyzing their development. To quickly react to new attack types, it also helps to know who the important players are and what new tools they offer. For instance, antivirus firms should keep an eye on companies that offer tools for evading detection and tracking down new malware types.

To learn more about how people's hacking actions and ideas may be influenced, conversations within these online forums might be researched. Furthermore, it demonstrates the considerable amount of hacking knowledge that can be used to address the key issues society is currently facing with cybersecurity and the shortage of trained personnel. By interacting with these groups, it would be able to direct young people away from criminal activity and toward the increasing number of genuine cybersecurity job openings that are vacant.

1. Acknowledgments

We would like to thank our professor for providing us with the opportunity to do a study on this topic. We would also like to thank all the people with whose research papers, we were able to compile our work.

##### References

1. Trend Micro. (n.d.) Trend Micro Security News. “Cybercriminal Underground Economy Series.” Last accessed on 26 March 2020 at <https://www.trendmicro.com/vinfo/us/security/news/cybercriminal-underground-economy-series>.
2. A. Caines, S. Pastrana, A. Hutchings, and P. J. Buttery, “Automatically identifying the function and intent of posts in underground forums,” Crime Sci, vol. 7, no. 1, p. 19, Dec. 2018, doi: 10.1186/s40163-018-0094-4.
3. J. McAlaney, S. Hambidge, E. Kimpton, and H. Thackray, “Knowledge is power: An analysis of discussions on hacking forums,” in 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Genoa, Italy, Sep. 2020, pp. 477–483. doi: 10.1109/EuroSPW51379.2020.00070.
4. A. Caines, S. Pastrana, A. Hutchings, and P. Buttery, “Aggressive language in an online hacking forum,” in Proceedings of the 2nd Workshop on Abusive Language Online (ALW2), Brussels, Belgium, 2018, pp. 66–74. doi: 10.18653/v1/W18-5109.
5. Brian O’Connor. (9 May 2018). Experian. “Cybercrime: The $1.5 Trillion Problem.” Last accessed on 28 March 2020 at https:// www.experian.com/blogs/ask-experian/cybercrime-the-1-5-trillion-problem/.I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963.
6. <https://www.csoonline.com/article/3340049/how-much-does-it-cost-to-launch-a-cyberattack.html>
7. <https://www.nibusinessinfo.co.uk/content/common-cyber-security-measures>
8. https://hbr.org/2017/04/8-ways-governments-can-improve-their-cybersecurity
9. <https://blog.feedspot.com/hacking_forums/>
10. <https://socradar.io/top-5-underground-hacker-forums-that-are-accessible-via-your-web-browsers-such-as-google-chrome-firefox-and-internet-explorer/>
11. https://www.makeuseof.com/tag/find-active-onion-sites/
12. Van Wegberg, R., Tajalizadehkhoob, S., Soska, K., Akyazi, U., Ganan, C. H., Klievink, B., Christin, N., and Van Eeten, M. (2018). Plug and prey? measuring the commoditization of cybercrime via online anonymous markets. In 27th USENIX security symposium (USENIX security 18).
13. International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)