IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 5, May 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205316 |

Dark Web and Cyber Extortion

Satish Sudarshan Pawar, Mihir Rajesh Narvekar, Prof. Supriya Santosh Surve

Department of MCA, Finolex Academy of Management and Technology, Ratnagiri, Maharashtra, India

ABSTRACT: The Dark Web, a hidden part of the Internet not accessible via search engines and requiring the Tor browser, has become a breeding ground for illegal activities and sophisticated cyberattacks. Its concealed network and anonymity facilitate well-planned, coordinated malicious activities, with cybersecurity experts noting a significant rise in online criminal activities. These crimes range from data breaches and ransomware attacks to black markets, mafia operations, and terrorism, affecting individuals and nations alike. Ensuring data privacy and secrecy has thus become a critical challenge. This paper reviews various attacks and attack patterns prevalent on the Dark Web, introducing a unique trilogies classification system for these threats. It also examines current threat detection techniques and their limitations for anonymity services like Tor, I2P, and Freenet, identifying significant vulnerabilities. Additionally, the research delves into the dynamics of cyber extortion within the Dark Web, exploring the mechanisms, key players, and motivations behind these activities. The study combines qualitative and quantitative analyses to trace the evolution of cyber extortion tactics, scrutinizing underground forums, marketplaces, and communication channels. It investigates the tools and techniques used by cybercriminals, from ransomware attacks to DDoS threats, and examines the economic aspects of cyber extortion. Furthermore, the paper highlights the challenges faced by law enforcement in tracking and prosecuting cyber extortionists, emphasizing the broader implications of cyber extortion on national security, privacy, and public trust in digital platforms. It also discusses potential countermeasures and policy interventions to mitigate the impact of cyber extortion, underscoring the need for collaborative efforts between governments, industry stakeholders, and cybersecurity experts.

KEYWORDS: Dark Web, Cyber Extortion.

I. INTRODUCTION

As the 21st century is a digital era, more information is online, allowing people to share and connect globally with just a click. The web visible to ordinary users is a vast resource, but it only represents about 4% of the entire internet. The remaining 96%, known as the deep web, is hidden and non-indexed. A subset of the deep web, the dark web, is mainly used for illegal activities.

Studies show that 57% of activities on the dark web are illegal, including data breaches, drug trafficking, pornography, and human trafficking. In 2018, the University of Surrey reported that cybercrimes generated approximately $1.5 trillion in revenue, indicating that these crimes are becoming more frequent and aggressive.

The Dark Web represents a clandestine realm of the internet, accessible only through specialized software like Tor, where anonymity prevails, fostering illegal activities. It operates on overlay networks using encryption and routing techniques to conceal users' identities and locations, creating a breeding ground for cyber extortion. Cyber extortion manifests in various forms, such as ransomware attacks, distributed denial-of-service (DDoS) threats, and data breaches. Ransomware attacks involve malicious software that encrypts victims' files or systems, rendering them inaccessible until a ransom is paid. DDoS attacks flood a target's network with traffic, causing disruption unless payment is made to cease the attack. Data breaches involve stealing sensitive information, which is then used to extort money or sold on underground markets.

Cyber extortionists often demand payment in cryptocurrencies like Bitcoin, which offer anonymity and are hard to trace, complicating law enforcement efforts. The global nature of the internet allows cybercriminals to operate across borders, further challenging efforts to combat cyber extortion. Victims face significant financial losses, including ransom payments, remediation costs, and potential fines for regulatory non-compliance. Organizations may also suffer reputational damage, loss of customer trust, and legal repercussions from data breaches. Individuals targeted by cyber extortion may experience emotional distress and privacy violations.

To mitigate the risks of cyber extortion, organizations and individuals must prioritize cybersecurity measures. This includes regular software updates, strong encryption, and multi-factor authentication. Maintaining offline backups of critical data can mitigate the impact of ransomware attacks. Public awareness about the dangers of the Dark Web and

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205316 |

cyber extortion is essential to empower individuals to recognize and respond effectively to threats. Collaboration between governments, law enforcement agencies, and the private sector is crucial to combat cybercrime and safeguard against the ever-evolving tactics of cyber extortionists.

Darkweb and phishing, cybercrime

The Darkweb is often associated with cybercrime, including phishing attacks. Recent studies have detected phishing and other malicious activity in the Darkweb [1]. For example, developing machine learning techniques and data analytics tools can help identify and track phishing campaigns and other forms of cybercrime [2]. Another research has focused on using active probing-based schemes and data analytics to investigate malicious fast-flux web-cloaking-based domains, often used in phishing attacks [3]. These schemes involve automated tools to probe suspected domains and gather information about their activity and characteristics.

Darkweb and botnet, malware

The Darkweb is often used as a platform for distributing botnets and malware, which are tools that can be used for various malicious purposes, including distributed denial of service (DDoS) attacks, spamming, and identity theft. One example of recent research in this area is the analysis of a '/0′ stealth scan from a botnet [4]. This study examined the characteristics and behavior of a particular type of botnet and attempted to identify the motivations and tactics of the attackers behind it. Other research has focused on identifying the most influential suspicious domains in the Tor network, a network of servers that can be used to access the Darkweb [5]. This research used a machine learning technique called “ToRank” to identify and rank the most influential domains based on their activity and connections to other domains [6]. Research has also focused on detecting botnet activities within large-scale Darknets by analyzing extensive data from the Dark web to identify patterns and trends. Additionally, studies have explored the use of Dark web crawlers to uncover suspicious and malicious websites on the Dark web.

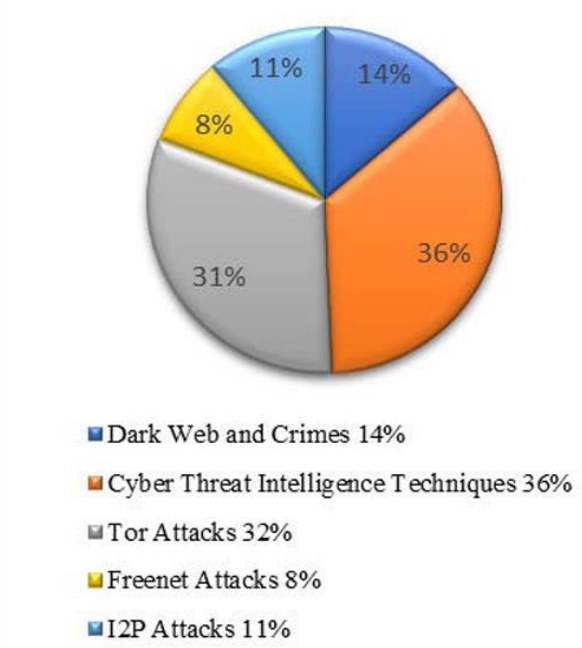
II. LITERATURE REVIEW

This article aims to provide a thorough analysis of dark web anonymity, highlighting its key aspects. We offer a brief overview of dark web tools, the types of crimes prevalent on the dark web, threat intelligence techniques for crime detection, and attacks on the dark web along with their countermeasures. Collecting and organizing the most pertinent literature presents a significant initial challenge for this review. Our primary aim was to compile this literature and offer a collective overview of various threats, their methods of implementation, and the attack patterns employed by cybercriminals. This analysis aims to provide researchers with a foundation to design prototypes for mitigating these threats. The approach to this was to search with keywords in central databases, go back and forth, i.e., to review citations and review material citing those critical articles. To gather the literature for our analysis, various databases and journals are used to collect academic indexed literature, namely IEEE Xplore, ACM digital library, Scopus, Springer, Science Direct, and Google Scholar. The broad keywords initially used in the searches were dark web or darknet, as these terms referred to the investigations central concept. The most popular dark web browser was added in the search, and thus the keywords Tor, I2P, and Freenet. The search focused on articles published between 2011 and 2021. To explore the themes of interest, the main keywords (dark web, Tor, I2P, Freenet) were paired with additional terms such as markets, cybercrime, Tor hidden services, patterns, threat intelligence methods, threat landscape, attack anonymity, or deanonymization, each added one at a time. These different keywords were added to allow for a more in-depth discussion of each aspect of the topic. This keyword search yielded a list of 150 journal articles and conference papers. The lists have identified the documents published in leading journals through the journal ranking by CORE 2020. Papers were then entered manually for greater relevance by selecting only those focused on the topics and peripherally relevant. The final list was composed of 79 articles categorized in 5 different areas mentioned in Figure 1. In our review process, almost 50% of our literature review focuses on attacks, 36% on threat intelligence techniques, and 14% on the dark web anonymity and crimes taking place in the dark web. However, there is a lack of literature on mitigating techniques against those attacks. It should be noted that in this framework, many elements are not restricted to what is depicted The first category discusses the anonymity of the dark web and crimes occurring because of this anonymity. We have mainly focused on the anonymity of Tor, I2P, and Freenet on the dark web. The second category examines the detection approaches for crimes, and the third category discusses the attacks on the dark web. These attacks are made mainly by two groups of people; one group is by law enforcement(LE) agencies to deanonymize the criminals and the second group is by the criminals to do malicious activities like hacking, ransomware information leakage, etc. Human and drug trafficking, child pornography, Terrorism, bitcoin, and money laundering are also included.[7]

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205316 |



1. Cyber Extortion:
Cyber extortion involves the use of technology to threaten individuals or organizations with harm, typically in exchange for money or other concessions. This malicious activity includes tactics such as ransomware attacks, where cybercriminals encrypt data and demand a ransom for its release; Distributed Denial of Service (DDoS) attacks, which overwhelm online services with excessive traffic, causing disruptions until payment is made; data breaches, where sensitive information is stolen and threatened to be released unless a ransom is paid; and threats to expose compromising information unless demands are met. The motives behind cyber extortion are primarily financial, as cybercriminals seek to profit by exploiting the fear of loss or damage to data and operations. However, some attackers are driven by political agendas, aiming to influence decisions or destabilize governments, while others, such as hacktivist groups, use cyber extortion to advance ideological beliefs and social causes.

2. Dark Web Marketplaces for Cyber Extortion:
The dark web plays a crucial role in facilitating cyber extortion by providing anonymity to cybercriminals, enabling them to conduct illegal activities without easily being traced. This hidden part of the internet hosts numerous marketplaces where cybercriminals buy and sell tools and services necessary for extortion activities. Popular dark web marketplaces offer sophisticated platforms for transactions involving ransomware-as-a-service (RaaS), where even individuals with limited technical skills can launch ransomware attacks by purchasing or renting malware from more skilled cybercriminals. These marketplaces have become highly sophisticated, mirroring legitimate e-commerce sites with features such as customer reviews, escrow services, and professional customer support. The professionalization of cyber extortion schemes is evident in the organized and business-like operations of these marketplaces, making it easier for a wider range of individuals to engage in cyber extortion activities, thereby amplifying the threat.

3. Impact and Consequences:
Cyber extortion has far-reaching consequences, including significant financial costs, reputational damage, and psychological effects on victims. Financially, it imposes direct costs like ransom payments and indirect costs such as downtime, recovery expenses, legal fees, and increased insurance premiums. Reputationally, it tarnishes the image of affected businesses, leading to a loss of trust and credibility among customers, partners, and stakeholders, and causing long-term damage to the brand's image. Psychologically, victims experience stress, anxiety, and fear of future attacks, with individuals feeling distressed by privacy invasions and business leaders facing burnout and decreased morale. The profound impact on financial stability, reputation, and mental health underscores the need for robust cybersecurity measures and effective crisis management strategies.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205316 |

4. Mitigation and Prevention Strategies:
Mitigating and preventing cyber extortion requires a multi-faceted approach that includes robust cybersecurity measures, proactive threat intelligence, and comprehensive incident response planning. Implementing security controls such as firewalls, antivirus software, and intrusion detection systems is essential for protecting against unauthorized access and malware. Threat intelligence plays a critical role in identifying and mitigating threats by monitoring dark web forums and marketplaces, allowing organizations to anticipate and counteract potential attacks. Developing comprehensive incident response plans is vital for quickly detecting, containing, and recovering from cyber extortion incidents, involving clear procedures, established roles, regular drills, and effective communication strategies. Integrating these strategies enhances organizational resilience against cyber extortion and minimizes its potential impact.

III. PROBLEM DEFINITION

The internet has revolutionized communication and information access. However, a hidden layer known as the dark web exists, accessible only through specialized This anonymity fosters criminal activity, including cyber extortion – the act of threatening to release damaging information or disrupt operations unless a ransom is paid. This paper investigates the convergence of these phenomena, highlighting the critical challenges they pose.

Steal sensitive data: Through various techniques like phishing, malware attacks, and data breaches, criminals can acquire personal information, financial records, or confidential business data.

Facilitate extortion schemes: The stolen data becomes leverage for extortion. Criminals threaten to publish the data online, sell it on dark web marketplaces, or disrupt critical systems unless the victim submits to their demands.

IV. OBJECTIVE & SCOPE

Objective of Dark Web and Cyber Extortion
Monetary Gain: The primary objective of cyber extortion is financial profit. Cybercriminals use various methods to extract money from individuals and organizations, including ransomware attacks, where they encrypt data and demand a ransom for its release.

Anonymity: The dark web provides a platform for cybercriminals to operate with a high degree of anonymity. This makes it difficult for law enforcement to track and apprehend them, thus facilitating illegal activities.

Data Breach and Sale: Stolen data, such as personal information, credit card details, and proprietary business information, is often sold on dark web marketplaces. This data can be used for identity theft, financial fraud, and further extortion.

Espionage and Competitive Advantage: Corporate espionage is another objective. Cyber extortion can involve stealing trade secrets and sensitive information from competitors and selling it to rival companies.

Political and Ideological Motives: In some cases, the objective may be to disrupt or undermine entities for political or ideological reasons. Hacktivist groups might use cyber extortion to draw attention to their causes or destabilize institutions they oppose.

Scope of Dark Web and Cyber Extortion :
Ransomware Attacks: One of the most prevalent forms of cyber extortion, ransomware attacks involve infecting a victim's system with malware that encrypts files, followed by a demand for ransom to decrypt the data.

DDoS Attacks: Distributed Denial of Service (DDoS) attacks involve overwhelming a network with traffic to render it unusable. Attackers then demand payment to stop the attack.

Phishing and Spear Phishing: These techniques involve tricking individuals into providing sensitive information (like login credentials) or installing malware. The stolen data can then be used for further extortion.

Data Breaches: Cybercriminals infiltrate networks to steal data, which is then used to blackmail organizations, threatening to release sensitive information if a ransom is not paid.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205316 |

Dark Web Marketplaces: These platforms facilitate the sale of illegal goods and services, including malware, hacking tools, and stolen data. They also offer services like renting botnets for DDoS attacks or hiring hackers for specific tasks.

Exploit Kits: These are software tools sold on the dark web that cybercriminals can use to find and exploit vulnerabilities in systems and networks.

Extortion-as-a-Service (EaaS): Some dark web actors offer extortion services for hire. This can include launching ransomware attacks or DDoS attacks on behalf of clients.

Criminal Networks and Partnerships: The dark web fosters a collaborative environment for cybercriminals, where they can form networks and partnerships to enhance their capabilities and reach.
The Intersection:
The dark web plays a crucial role in cyber extortion by providing a platform for:
Selling stolen data: Extortionists can purchase personal information like credit cards or medical records on dark web marketplaces.
Anonymous communication: Extortionists can use dark web forums or chat rooms to contact victims and negotiate ransoms without revealing their identity.
Advertising extortion services: Some dark web marketplaces even host listings for extortion-as-a-service, where criminals offer to carry out extortion attacks for a fee.

V. RESEARCH METHODOLOGY

Researching the dark web and cyber extortion presents unique challenges due to the clandestine nature of these activities. Here's a breakdown of potential methodologies:
1. Data Collection
Traditional methods like surveys or interviews won't work. Here are some alternative approaches:
Web Scraping (with Caution): Develop specialized crawlers to gather data from dark web forums, marketplaces, and chat rooms. This requires expertise in anonymity tools and ethical considerations to avoid scraping illegal content.
Law Enforcement Collaboration: Partner with law enforcement agencies for access to seized dark web data and insights into ongoing investigations.
Public Data Sources: Analyze reports from cybersecurity firms, dark web monitoring companies, and law enforcement publications to understand trends and tactics.
Social Media Analysis: Monitor specific hashtags or keywords on social media platforms that might be used by cybercriminals or victims to indirectly gather information.

2. Data Analysis Techniques
Text Analysis: Techniques like Natural Language Processing (NLP) can be used to analyze scraped data from forums and chats. Identify keywords, sentiment analysis, and topic modeling can reveal trends in extortion methods, target victim profiles, and communication patterns.
Network Analysis: Analyze connections between users on dark web platforms to understand how cybercriminals collaborate and organize. This can help identify key players and disrupt criminal networks.
Machine Learning (ML): Train ML models to identify indicators of compromise (IOCs) associated with cyber extortion attempts. This could include suspicious email patterns, language used in extortion threats, or specific malware signatures.

3. Ethical Considerations
Anonymity and Legality: Respect user anonymity on the dark web when scraping data. Avoid collecting personally identifiable information (PII).
Data Provenance: Clearly document the source and legality of all collected data.
Lawful Access: Ensure all data collection adheres to relevant laws regarding electronic surveillance and data privacy.

4. Additional Considerations
Security: Researchers need robust security measures to protect themselves from malware, phishing attacks, or other threats present on the dark web. Utilize anonymized access methods like Tor with strong encryption.
Interdisciplinary Approach: Combine expertise from cybersecurity, social sciences, and computer science for a holistic understanding of the phenomenon

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205316 |

VI. ANALYSIS AND FINDINGS

Studies reveal a disturbing trend:
Growing sophistication: Extortion tactics are becoming more targeted and personalized, increasing the pressure on victims to pay.
Rise of Ransomware-as-a-Service (RaaS): This model allows less-skilled actors to launch sophisticated attacks, further democratizing cyber extortion.
Financial Losses: Businesses and individuals incur significant financial losses due to extortion payments and the disruption caused by attacks.
Reputational Damage: Data breaches and extortion attempts can severely damage an organization's reputation.

VII. LIMITATIONS & FUTURE SCOPE

A) Anonymity and Detection Challenges:
Encryption and Anonymity: Tools like Tor and cryptocurrencies obscure the identities of users, making it difficult for law enforcement to trace and apprehend cybercriminals.
Limited Surveillance: Traditional surveillance techniques are less effective on the dark web due to its decentralized and encrypted nature.

B) Jurisdictional Issues:
Cross-Border Crimes: Cyber extortion often involves perpetrators and victims in different countries, complicating legal proceedings and enforcement actions.
Varying Legal Frameworks: Different countries have diverse laws and levels of enforcement, making international cooperation challenging.

C) Rapid Evolution of Threats:
Adaptability of Attackers: Cybercriminals continuously adapt their techniques to bypass existing security measures and exploit new vulnerabilities.
Proliferation of Ransomware-as-a-Service (RaaS): The availability of ransomware tools for hire enables even low-skilled criminals to launch sophisticated attacks.

D) Victim Response and Reporting:
Underreporting: Many victims do not report cyber extortion incidents due to fear of reputational damage, regulatory repercussions, or lack of trust in law enforcement.
Payment of Ransoms: Some victims opt to pay ransoms quickly to restore operations, inadvertently funding and encouraging further criminal activities.

E) Technological and Resource Constraints:
Resource Limitations: Law enforcement agencies often lack the resources and technical expertise to effectively combat dark web activities and cyber extortion.
Complexity of Attribution: Identifying and attributing cyber attacks to specific individuals or groups remains a complex and resource-intensive process.

VIII. CONCLUSION

Cyber-extortion is a significant yet under-addressed problem, becoming increasingly professional and dangerous. Identifying or locating cyber-extortionists, who often operate internationally, is challenging, and victims rarely recover damages due to the extortionists' limited financial resources. Businesses with poorly protected information systems are attractive targets, facing substantial liability risks. Improved communication between attorneys, IT professionals, and executives is crucial to effectively address cybersecurity incidents. This paper simplifies various cyber-attacks and detection methods, highlighting existing work, loopholes, deficits, and areas for improvement. Further research is needed to investigate crime ratios on the dark web and its relationship with the crypto market, develop AI techniques for large-scale, real-time threat detection and prevention, and create a comprehensive monitoring system for forums, marketplaces, websites, and traffic. Collaboration between law enforcement, researchers, and white-hat hackers is essential to securing the dark web. Future research should also focus on assessing the effectiveness of denial-of-service attacks on Tor, I2P, and Freenet, and performing traceback attacks on peer-to-peer systems while comparing traffic attacks across different anonymity tools

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205316 |

REFERENCES

[1] X. Jie, L. Haoliang, J. Ao A new model for simultaneous detection of phishing and Darknet websites 2021 7th International Conference on Computer and Communications (ICCC), IEEE (2021), pp. 2002-2006 View at publisher CrossRefView in ScopusGoogle Scholar

[2] I.N.V.D. Naveen, K. Manamohana, R. Verma Detection of malicious URLs using machine learning techniques Int. J. Innovative Technol. Explor. Eng., 8 (4S2) (2019), pp. 389-393 View in ScopusGoogle Scholar

[3] Z. Guo, Y. Guan Active probing-based schemes and data analytics for investigating malicious fast-flux web-cloaking based domains 2018 27th International Conference on Computer Communication and Networks (ICCCN), IEEE (2018), pp. 1-9 View PDFView articleGoogle Scholar

[4] A. Dainotti, A. King, K.C. Claffy, F. Papale, A. Pescapé Analysis of a"/0" stealth scan from a botnet Proceedings of the 2012 Internet Measurement Conference (2012), pp. 1-14 View at publisher CrossRefGoogle Scholar

[5] M.W. Al-Nabki, E. Fidalgo, E. Alegre, L. Fernández-Robles Torank: identifying the most influential suspicious domains in the tor network Expert Syst. Appl., 123 (2019), pp. 212-226 View PDFView articleView in ScopusGoogle Scholar

[6]T. Ban, L. Zhu, J. Shimamura, S. Pang, D. Inoue, K. Nakao Detection of botnet activities through the lens of a large-scale Darknet Neural Information Processing: 24th International Conference, ICONIP 2017 (2017) Google Scholar

[7] The Anonymity of the Dark Web: A Survey January 2022 IEEE Access 10(6):1-1 January 2022 10(6):1-1 DOI:10.1109/ACCESS.2022.3161547 License CC BY 4.0

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details