Journal of Neonatal Surgery
ISSN(Online): 2226-0439
Vol. 14, Issue 28s (2025)
https://www.jneonatalsurg.com

OPEN ACCESS

Cyber Extortion In Dark Web

Krishna Ashokkumar Sharma[1*], Devesh Ravindra Ekhande[2], Harshit Anil Agrawal[3], Nikhil Rajendra Ghinmine[4], Arpan[5], Prof. Vivek Dave[6]

[*1]Master of computer application Parul University, Vadodara, Gujarat.
Email ID: 2305112140043@paruluniversity.ac.in
[2]Master of computer application Parul University, Vadodara, Gujarat.
Email ID: 2305112120041@paruluniversity.ac.in
[3]Master of computer application Parul University, Vadodara, Gujarat.
Email ID: 2305112110106@paruluniversity.ac.in
[4]Master of computer application Parul University, Vadodara, Gujarat.
Email ID: 2305112120047@paruluniversity.ac.in
[5]Master of Computer Science Parul university, Vadodara, Gujarat.
Email ID: 2305102130005@paruluniversity.ac.in
[6]Head of Department at Parul University of Engineering & Technology-MCA Vadodara, Gujarat,
Email ID: vivek.dave@paruluniversity.ac.in

Cite this paper as: Krishna Ashokkumar Sharma, Devesh Ravindra Ekhande, Harshit Anil Agrawal, Nikhil Rajendra Ghinmine, Arpan, Prof. Vivek Dave, (2025) Cyber Extortion In Dark Web. *Journal of Neonatal Surgery*, 14 (28s), 933-939.

ABSTRACT
The Dark Web has surfaced as a critical mecca for cyber highway robbery, enabling cybercriminals to exploit encryption technologies similar as Tor, I2P, and Freenet to conduct lawless conditioning anonymously. This paper examines the growing trouble of cyber highway robbery, assaying crucial attack styles, perpetrators, and provocations. Cyber highway robbery takes multiple forms, including ransomware, Distributed Denial- of- Service(DDoS) attacks, data breaches, and blackmail, with cybercriminals using underground forums, translated dispatches, and cryptocurrency to shirk discovery. To classify these pitfalls, the study introduces a triplets frame comprising Technological Extortion(e.g., ransomware and DDoS- for-hire), Data Manipulation Extortion(e.g., data exposure and revision), and Cerebral highway robbery(e.g., sextortion and deepfake blackmail). The exploration explores the elaboration of highway robbery ways, from phishing swindles to automated Ransomware- as-a- Service(RaaS) and DDoS- for- Hire operations, with cryptocurrency playing a pivotal part in rescue payments and plutocrat laundering.Despite advancements in network business analysis, AI- driven anomaly discovery, and legal interventions, combating cyber highway robbery remains a challenge due to jurisdictional complications and anonymized felonious networks. This study highlights the need for amulti-faceted approach, including zero- trust security fabrics, transnational legal cooperation, and mindfulness juggernauts. By assaying real- world cases of REvil, DarkSide, and LockBit, this paper underscores the urgency of global intelligence- sharing and forensic advancements to alleviate cyber highway robbery pitfalls.

Keywords: *Cyber Extortion, Dark Web*

1. INTRODUCTION

As the 21st century is a digital period, further information is online, allowing people to partake and connect encyclopedically with justa click. The web visible to ordinary druggies is a vast resource, but it only represents about 4 of the entire internet. Theremaining 96, known as the deep web, is hidden andnon-indexed. A subset of the deep web, the dark web, is substantially used for illegal conditioning. borders, further grueling sweats to combat cyber highway robbery. Victims face significant fiscal losses, including rescue payments, remediation costs, and implicit forfeitures for nonsupervisorynon-compliance. Organizations may also suffer reputational damage, loss of client trust, and legal impacts from data breaches. individualities targeted by cyber highway robbery may witness emotional torture and sequestration violations.To alleviate the pitfalls of cyber highway robbery, associations and individualities must prioritize cybersecurity measures. This includes regular software updates, strong encryption, andmulti-factor authentication. Maintaining offline backups of critical data can alleviate

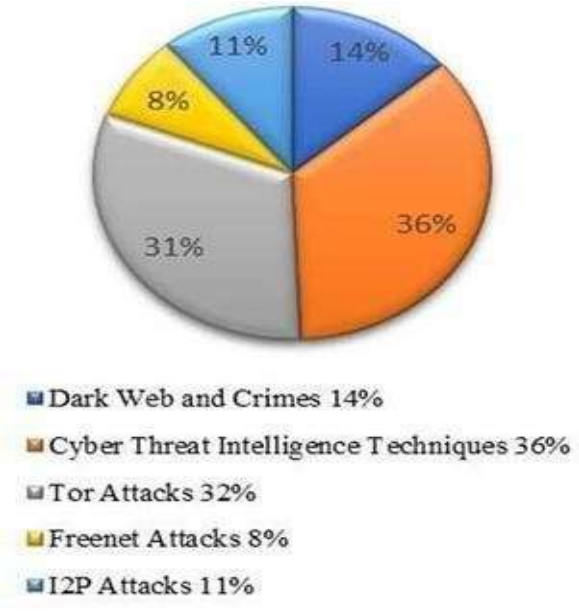
the impact of ransomware attacks. Public mindfulness about the troubles of the Dark Web and cyber highway robbery is essential to empower individualities to fete and respond effectively to pitfalls. Collaboration between governments, law enforcement agencies, and the private sector is pivotal to combat cybercrime and safeguard against the ever- evolving tactics of cyber extortionists.Studies show that 57 of conditioning on the dark web are illegal, including data breaches, medicine trafficking, pornography, and mortal trafficking. In 2018, the University of Surrey reported that cybercrimes generated roughly$ 1.5 trillion in profit, indicating that these crimes are getting more frequent and aggressive.The Dark Web represents a covert realm of the internet, accessible only through specialized software like Tor, where obscurity prevails, fostering illegal conditioning. It operates on overlay networks using encryption and routing ways to conceal druggies' individualities and locales, creating abreeding ground for cyber extortion.Cyber extortionmanifests in colorful forms, similar as ransomware attacks, distributed denial- of- service(DDoS) pitfalls, and data breaches. Ransomware attacks involve vicious software that encrypts victims' lines or systems, rendering them inapproachable until a rescue is paid. DDoS attacks submerge a target's network with business, causing dislocation unless payment is made to cease the attack. Data breaches involve stealing sensitive information, which is also used to wring plutocrat or vended on underground markets.Cyber extortioners frequently demand payment in cryptocurrencies like Bitcoin, which offer obscurity and are hard to trace, complicating law enforcement sweats. The global nature of the internet allows cybercriminals to operate across. Dark web and phishing, cybercrime The Dark web is frequently associated with cybercrime, including phishing attacks. Recent studies have detected phishing and other vicious exertion in the Dark web(1). For illustration, developing machine literacy ways and data analytics tools can help identify and track phishing juggernauts and other forms of cybercrime(2). Another exploration has concentrated on using active delving- grounded schemes and data analytics to probe vicious fast- flux web- cloaking grounded disciplines, frequently used in phishing attacks(3). These schemes involve automated tools to probe suspected disciplines and gather information about their exertion and characteristics. Darkweb and botnet, malware The Darkweb is frequently used as a platform for distributing botnets and malware, which are tools that can be used for colorful vicious purposes, including distributed denial of service(DDoS) attacks, spamming, and identity theft. One illustration of recent exploration in this area is the analysis of a'/ 0 covert checkup from a botnet(4). This study examined the characteristics and geste of a particular type of botnet and tried to identify the provocations and tactics of the bushwhackers behind it. Other exploration has concentrated on relating the most influential suspicious disciplines in the Tor network, a network of waiters that can be used to pierce the Dark web(5). This exploration used a machine learning fashion called " To Rank " to identify and rank the most influential disciplines grounded on their exertion and connections to other disciplines(6). Research has also concentrated on detecting botnet conditioning within large- scale Darknets by assaying expansive data from the Dark web to identify patterns and trends. also, studies have explored the use of Dark web dawdlers to uncover suspicious and vicious websites on the Dark web.

2. LITERATURE REVIEW

This composition aims to give a thorough analysis of dark web obscurity, pressing its crucial aspects. We offer a brief overview of dark web tools, the types of crimes current on the dark web, trouble intelligence ways for crime discovery, and attacks on the dark web along with their countermeasures. Collecting and organizing the most material literature presents a significant original challenge for this review. Our primary end was to collect this literature and offer a collaborative overview of colorful pitfalls, their styles of perpetration, and the attack patterns employed by cybercriminals. This analysis aims to give experimenters with a foundation to design prototypes for mollifying these pitfalls. The approach to this was to search with keywords central databases, go back and forth, i.e., to review citations and review material citing those critical papers. To gather the literature for our analysis, colorful databases and journals are used to collect academic listed literature, videlicet IEEE Xplore, ACM digital library, Scopus, Springer, Science Direct, and Google Scholar. The broad keywords originally used in the quests were dark web or darknet, as these terms appertained to the examinations central conception. The most popular dark web cybersurfer was added in the hunt, and therefore the keywords Tor, I2P, and Freenet. The hunt concentrated on papers published between 2011 and 2021. To explore the themes of interest, the main keywords(dark web, Tor, I2P, Freenet) were paired with fresh terms similar as requests, cybercrime, Tor retired services, patterns, trouble intelligence styles, trouble geography, attack obscurity, 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 content. This keyword hunt yielded a list of 150 journal papers and conference papers. The lists have linked the documents published in leading journals through the journal ranking by CORE 2020. Papers were also entered manually for lesser applicability by opting only those concentrated on the motifs and peripherally applicable. The final list was composed of 79 papers distributed in 5 different areas mentioned in Figure 1. In our review process, nearly 50 of our literature review focuses on attacks, 36 on trouble intelligence ways, and 14 on the dark web obscurity and crimes taking place in the dark web. still, there's a lack of literature on mitigating ways against those attacks. It should be noted that in this frame, numerous rudiments are n't confined to what's depicted The first order discusses the obscurity of the dark web and crimes being because of this obscurity. We've substantially concentrated on the obscurity of Tor, I2P, and Freenet on the dark web. The alternate order examines the discovery approaches for crimes, and the third order discusses the attacks on the dark web. These attacks are made substantially by two groups of people; one group is by law enforcement (LE) agencies to deanonymize the culprits and the alternate group is by the culprits to do vicious conditioning like hacking, ransomware information leakage, etc. mortal and medicine trafficking, child pornography,

Terrorism, bitcoin, and plutocrat laundering are also included.(7) 1. Cyber Extortion Cyber highway robbery involves the use of technology to hang individualities or associations with detriment, generally in exchange for plutocrat or other as ransomware attacks, where cybercriminals cipher data and demand a rescue for its release; Distributed Denial of Service(DDoS) attacks, which overwhelm online services with inordinate business, causing dislocations until payment is made; data breaches, where sensitive information is stolen and hovered to be released unless a rescue is paid; and pitfalls to expose compromising information unless demands are met. The motives behind cyber highway robbery are primarily fiscal, as cybercriminals seek to benefit by exploiting the fear of loss or damage to data and operations. still, some bushwhackers are driven by political dockets, aiming to impact opinions or destabilize governments, while others, similar as hacktivist groups, use cyberextortion to advideological beliefs and social causes. 2. Dark Web commerce for Cyber Extortion The dark web plays a pivotal part in easing cyber highway robbery by furnishing obscurity to cybercriminals, enabling them to conduct illegal conditioning without fluently being traced. This retired part of the internet hosts multitudinous commerce where cybercriminals buy and vend tools and services necessary for highway robbery conditioning. Popular dark web commerce offer sophisticated platforms for deals involving ransomware- as- a-service (RaaS), where indeed individualities with limited specialized chops can launch ransomware attacks by copping or renting malware from further professed cybercriminals. These commerce have come largely sophisticated, mirroring licite-commerce spots with features similar as client reviews, escrow services, and professional client support. The professionalization of cyber highway robbery schemes is apparent in the organized and business- suchlike operations of these commerce, making it easier for a wider range of individualities to engage in cyber highway robbery conditioning, thereby amplifying the trouble. 3. Impact and Consequences Cyber highway robbery has far- reaching consequences, including significant fiscal costs, reputational damage, and cerebral goods on victims. Financially, it imposes direct costs like rescue payments and circular costs similar as time-out, recovery charges, legal freights, and increased insurance decorations. Reputationally, it tarnishes the image of affected businesses, leading to a loss of trust and credibility among guests, mates, and stakeholders, and causing long- term damage to the brand's image. Psychologically, victims experience stress, anxiety, and fear of unborn attacks, with individualities feeling worried by sequestration irruptions and business leaders facing collapse and dropped morale. The profound impact on fiscal stability, character, and internal health underscores the need for robust cybersecurity measures and effective extremity operation strategies.

against cyber highway robbery and minimizes its implicit impact. journal ranking by CORE 2020. Papers were also entered manually for lesser applicability by opting only those concentrated on the motifs and peripherally applicable. The final list was composed of 79 papers distributed in 5 different areas mentioned in Figure 1. In our review process, nearly 50 of our literature review focuses on attacks, 36 on trouble intelligence ways, and 14 on the dark web obscurity and crimes taking place in the dark web. still, there's a lack of literature on mitigating ways against those attacks. It should be noted that in this frame, numerous rudiments are n't confined to what's depicted The first order discusses the obscurity of the dark web and crimes being because of this anonymity. We've substantially concentrated on the obscurityof Tor, I2P, and Freenet on the dark web. The alternate order examines the discovery approaches for crimes, and the third order discusses the attacks on the dark web. These attacks are made substantially by two groups of people; one group is by law enforcement(LE) agencies to deanonymize the culprits and the alternate group is by the culprits to do vicious conditioning like hacking, ransomware information leakage, etc. mortal and medicine trafficking, child pornography, Terrorism, bitcoin, and plutocrat laundering are also included.(7)



Cyber Extortion Cyber highway robbery involves the use of technology to hang individualities or associations with detriment, generally in exchange for plutocrat or other as ransomware attacks, where cybercriminals cipher data and demand a rescue for its release; Distributed Denial of Service(DDoS) attacks, which overwhelm online services with inordinate business, causing dislocations until payment is made; data breaches, where sensitive information is stolen and hovered to be released unless a rescue is paid; and pitfalls to expose compromising information unless demands are met. The motives behind cyber highway robbery are primarily fiscal, as cybercriminals seek to benefit by exploiting the fear of loss or damage to data and operations. still, some bushwhackers are driven by political dockets, aiming to impact opinions or destabilize governments, while others, similar as hacktivist groups, use cyber extortion to advideological beliefs and social causes.

Dark Web commerce for Cyber Extortion The dark web plays a pivotal part in easing cyber highway robbery by furnishing obscurity to cybercriminals, enabling them to conduct illegal conditioning without fluently being traced. This retired part of the internet hosts multitudinous commerce where cybercriminals buy and vend tools and services necessary for highway robbery conditioning. Popular dark web commerce offer sophisticated platforms for deals involving ransomware- as-a-service(RaaS), where indeed individualities with limited specialized chops can launch ransomware attacks by copping or renting malware from further professed cybercriminals. These commerce have come largely sophisticated, mirroring licite-commerce spots with features similar as client reviews, escrow services, and professional client support. The professionalization of cyber highway robbery schemes is apparent in the organized and business- suchlike operations of these commerce, making it easier for a wider range of individualities to engage in cyber highway robbery conditioning, thereby amplifying the trouble.

Impact and Consequences Cyber highway robbery has far- reaching consequences, including significant fiscal costs, reputational damage, and cerebral goods on victims. Financially, it imposes direct costs like rescue payments and circular costs similar as time-out, recovery charges, legal freights, and increased insurance decorations. Reputationally, it tarnishes the image of affected businesses, leading to a loss of trust and credibility among guests, mates, and stakeholders, and causing long- term damage to the brand's image. Psychologically, victims experience stress, anxiety, and fear of unborn attacks, with individualities feeling worried by sequestration irruptions and business leaders facing collapse and dropped morale. The profound impact on fiscal stability, character, and internal health underscores the need for robust cybersecurity measures and effective extremity operation strategies.

Mitigation and Prevention Strategies Mitigating and precluding cyber highway robbery requires amulti-faceted approach that includes robust cybersecurity measures, visionary trouble intelligence, and comprehensive incident response planning. enforcing security controls similar as firewalls, antivirus software, and intrusion discovery systems is essential for guarding against unauthorized access and malware. trouble intelligence plays a critical part in relating and mollifying pitfalls by covering dark web forums and commerce, allowing associations to anticipate and offset implicit attacks. Developing comprehensive incident response plans is vital for snappily detecting, containing, and recovering from cyber highway robbery incidents, involving clear procedures, established places, regular drills, and effective communication strategies.

Integrating these strategies enhances organizational adaptability against cyber highway robbery and minimizes its implicit impact. web forums and commerce, allowing associations to anticipate and offset implicit attacks. Developing comprehensive incident response plans is vital for snappily detecting, containing, and recovering from cyber highway robbery incidents, involving clear procedures, established places, regular drills, and effective communication strategies. Integrating these strategies enhances organizational adaptability.

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. 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

3. 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 theconvergence 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.

4. OBJECTIVE ABD SCOPE

Objective of Cyber Extortion Dark Web and: 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 Cyber Extortion Dark Web and: 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. 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 we 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 market places. 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.

5. RESEARCH METHODOLOGY

Researching cyber extortion on the Dark Web presents challenges due to its covert nature. Traditional methods like surveys or interviews are ineffective, requiring alternative data collection approaches. Web scraping, with ethical precautions, can extract insights from dark web forums and marketplaces, while collaboration with law enforcement provides access to seized data and investigative findings. Public sources, such as cybersecurity reports and law enforcement publications, help track trends, while social media analysis monitors relevant discussions. Data analysis techniques include Natural Language Processing (NLP) for text analysis, network analysis to map criminal collaborations, and machine learning (ML) models to detect cyber extortion patterns. Ethical considerations are crucial, ensuring anonymity, data provenance, and legal compliance. Researchers must follow data privacy laws and avoid collecting personally identifiable information (PII). Security is also a key concern, requiring strong encryption and anonymized access to prevent exposure to cyber threats. A multidisciplinary approach integrating cybersecurity, social sciences, and computer science is essential for a comprehensive understanding of cyber extortion tactics and mitigation strategies.

6. ANALYSIS AND FINDING

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.

7. LIMITATIONS AND FUTURE SCOPE

A) Anonymity and Detection Challenges: LIMITATIONS & FUTURE SCOPE

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

8. 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

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 botne 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 To rank: identifying the most influential suspicious domains in the tor networkExpert 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