Tor Attack Studies: A Survey on Active and Passive Subject

Mohamad Amar Irsyad Mohd Aminuddin[1], Zarul Fitri Zaaba[1], Azman Samsudin[1], Nor Badrul Anuar Juma'at[2]

[1] School of Computer Sciences, Universiti Sains Malaysia, 11800 Pulau Pinang, Malaysia

[2] Faculty of Computer Science & Information Technology, Universiti Malaya, 50603 Kuala Lumpur, Malaysia

Abstract: Privacy is one of the important aspects that the Internet user would like to protect. The introduction of Tor as a tool for anonymous Internet access has attracted the attention of researchers worldwide. Various researchers had proposed an attack technique in order to challenge the anonymity properties provided by Tor to the Internet user. Due to a lack of adequate comprehension of the attacked subject utilized in the various Tor attack studies, this paper aims to classify and analyze the attacked subject on those studies. Our research goal is to review and analyze the attack subject practice and trends in the Tor research field. The knowledge obtained from this study will allow for better comprehension of the nature of the attacks executed on Tor and will be useful for researchers' guidance, especially in the context of practice and trends in attack subjects on Tor. Therefore, this study classified the attacked subject on Tor based upon 80 reviewed studies related to attacking the Tor. This classification had yielded several new substantial pieces of knowledge on the subject utilized in the Tor attack. It is revealed that most of the researchers had focused on monitoring the network traffic between the user and Entry OR, followed by malicious Exit OR and malicious Entry OR. In addition, various studies have been found to utilize more than one attack subject in attacking the Tor network.

Keywords: anonymity, attack, privacy, security, Tor.

托攻击研究：关于主动和被动主题的调查

摘要：隱私是互聯網用戶希望保護的重要方面之一。托作為匿名互聯網訪問工具的引入引起了全世界研究人員的關注。許多研究人員提出了一種攻擊技術，以挑戰托為互聯網用戶提供的匿名特性。由於對各種 Tor 攻擊研究中使用的受攻擊對象缺乏足夠的理解，本文旨在對這些研究中的受攻擊對象進行分類和分析。我們的研究目標是回顧和分析托研究領域的攻擊主題實踐和趨勢。從這項研究中獲得的知識將有助於更好地理解在托上執行的攻擊的性質，並將有助於研究人員的指導，特別是在托上攻擊對象的實踐和趨勢的背景下。因此，本研究根據 80 項與攻擊托 相關的審查研究對托上的攻擊對象進行了分類。這種分類產生了一些關於托攻擊中使用的主題的新的實質性知識。據透露，大多數研究人員都專注於監控用戶與入口洋蔥路由器之間的網絡流量，其次是惡意出口洋蔥路由器和惡意入口洋蔥路由器。此外，已經發現各種研究在攻擊 Tor 網絡時使用了不止一個攻擊對象。

关键词：匿名、攻擊、隱私、安全、托。

1. Introduction

In this modern age of communication, online privacy is one of the important aspects that the Internet user would like to protect. Despite the significant popularity of encrypted Internet traffic using the

Received: May 1, 2021 / Revised: May 6, 2021 / Accepted: August 17, 2021 / Published: September 30, 2021

About the authors: Mohamad Amar Irsyad Mohd Aminuddin, Zarul Fitri Zaaba, Azman Samsudin, School of Computer Sciences, Universiti Sains Malaysia, Pulau Pinang, Malaysia; Nor Badrul Anuar Juma'at, Faculty of Computer Science & Information Technology, Universiti Malaya, Kuala Lumpur, Malaysia

HTTPS (Hypertext Transfer Protocol Secure), this method only hides the message of communication traffic. The identity of the communication sender and recipient is still widely accessible, which leads to the reduction of privacy. The ease of identifying these communication entities by the adversary could be considered a major threat to Internet user privacy.

Hence, various works have been engaged to provide Internet users with a privacy-enhanced environment for online users. An anonymity platform named Tor (The Onion Router) was proposed to fulfill that necessity [1]. Since its inception in 2004, Tor has become one of the most popular privacy-enhancement tools for Internet users to protect their online identity. By using the Tor platform, two parties communicating with each other are very difficult to be associated with. This will allow an Internet user to hide their real identity (IP address) and prevent the third party from identifying with whom they are communicating. When a Tor user opens a Facebook website, the Facebook server cannot identify the actual IP address of that particular user. In addition, if an adversary is monitoring the user's Internet activity, the adversary would be unable to learn that the user had browsed the Facebook website because the Tor platform acts as the intermediary between the user and the Facebook server.

As one of the most popular anonymity tools on the Internet, Tor was used by over two million users in 2019 [2]. Consequently, it attracts many researchers' interest in challenging the anonymity properties provided by the Tor platform [3-4]. Numerous attack studies have been proposed out by these researchers in various angles and attacking scenarios.

Despite that work by [3], [4], [5], and [6] had made surveys on the Tor attack studies, there is still the aspect of Tor attack studies that are yet to be uncovered and remain ambiguous to this date. The attack subject utilized in various attack studies is yet to be classified and analyzed. Without an appropriate comprehension of the attacked subject utilized in those attack studies, the true nature of these attacks might be unable to be recognized.

On that account, this paper aims to classify and analyze the attacked subject on the Tor attack studies. The knowledge obtains from this study will allow for better comprehension of the nature of these Tor attack studies. In addition, knowledge on the trend and practice of attack subjects on various Tor studies will be useful for researchers' guidance in the future.

This paper is presented in seven main sections. Section 2 introduces the Tor working principle. Section 3 elaborates on the active subject use in Tor attack studies, while Section 4 elaborates on the passive subject. Section 5 classifies Tor attack studies with their respective attack subject. Section 6 analyses the practice and trend of the subject in Tor attack studies. Lastly, Section 7 will conclude this study.

2. Tor Background

Tor is developed based on onion routing architecture that operates on top of the regular Internet. The main principle of this architecture is that the network traffic is encapsulated into multiple layers of encryption that only be decrypted by Onion Router (OR) [1]. The OR is the entity in the Tor network that relays traffic from the Tor user to the actual recipient. When a Tor user communicates with a recipient, the network communication package will be encrypted into several layers and then forwarded through three ORs before it reaches the actual recipient. Each of the OR will decrypt an encryption layer to learn the destination to forward the traffic. Using this concept, only Entry OR (the first OR) knows the actual Tor user identity, and only the Exit OR (the third OR) knows the communication recipient. The Middle OR (the second OR) does not know the actual Tor user or communication recipient, but the Tor can provide anonymity to the Internet user. Fig. 1 illustrates the communication diagram between the Tor user and the destination. Green-line indicates that the network traffic is protected using the onion routing encryption, while red-line indicates regular internet traffic.

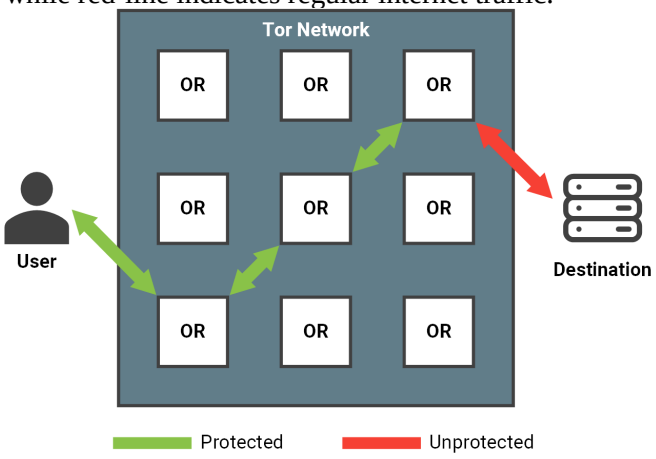

Fig. 1 Communication diagram in the Tor network

3. Active Attack Subject

To execute an attack on Tor, the attacker might choose the attack technique that requires the attacker to actively control a subject that will be utilized for the attack. The different subjects will require a different access method and provide different capabilities to the attacker to launch his attack. By reviewing the literature, the active attack subject could be classified into seven components. Generally, the attacker is expected to maliciously control these components by impersonating them as a legitimate component or corrupted the existing, legitimate component. The following is the discussion on these active attack subjects.

3.1. Client

The attacker used the Tor client software as the subject of an attack. The attacker impersonates a

normal Tor user to execute the attack that will allow for an attack that requires a legitimate Tor user as its subject. This attack subject is easiest to employ since anyone can download and install Tor client software. Though, it could be argued to be the least harmful compared to other malicious components as it does not give any unique advantage to the attacker as it only has access as a normal Tor user.

3.2. Entry OR

Attacker use Entry OR as the subject of an attack. The attacker controls an Entry OR to execute the attack, allowing for an attack that requires access to the Entry OR. The importance of Entry OR is that it does know the original sender of the communication message. By controlling the Entry OR, the attacker might have the possibility to learn the actual sender of the communication message. Despite that valuable information, it does not reveal any information on the actual destination of the traffic.

3.3. Middle OR

The attacker uses Middle OR as the subject of an attack, controlling Middle OR executing the attack that will allow for the attack that requires access to the Middle OR. Compared to the Entry OR, Middle OR does not know any valuable information such as the actual sender or recipient of a communication message. It only knows the Entry OR and Exit OR information. Nonetheless, it still might be useful if the attack is used for surveillance purposes [7].

3.4. Exit OR

Attacker use Exit OR as the subject of an attack. The attacker controls Exit OR to execute the attack, allowing for an attack that requires access to the Exit OR. By controlling the Exit OR, the attacker can learn the information on the actual destination of message communication. Despite the lack of information on the actual sender of the message communication, controlling the Exit OR might be useful for an attacker that wants to learn the actual destination of message communication or modify the traffic that will be sent to the actual destination [8].

3.5. Destination

Attacker impersonates as a legit destination of message communication. One of the major reasons to do this is to retrieve the information on the actual destination of the communication, which is supposed to be hidden on Tor [6]. Using a malicious destination, an attacker might employ a traceback technique that can leak the actual sender information [9]. An attacker might not need to set up a new malicious destination; instead, it can do so by injecting or manipulating the current existing components [9].

3.6. Autonomous System

An autonomous system refers to the collection of a connected Internet routing protocol. An attacker that managed to control a component of the autonomous system can control the network component that involves routing the Tor traffic. It could be an Internet Service Provider or Internet Exchange Point. The Tor traffic from the Tor's user to the actual destination might flow through one of these components controlled by an attacker. Although it could be argued as one of the most sophisticated active attack subjects, it could be useful for an attacker with the intention of mass surveillance or correlation between Tor's traffic [10].

3.7. Network Gateway

A network gateway refers to a local area network administrator administering the network connection between the Internet and its internal network user. It could be an entity on the campus network administrator or a company network administrator. While the autonomous system is only able to learn the public IP address of the user, the network gateway can correlate the communication between an Entry OR with an internal IP address of its network's user. This attack subject typically uses the network gateway to block users from accessing the Tor network [11-12].

4. Passive Attack Subject

In Tor attack studies, passive attack typically only monitors the Tor network traffic without modification or alteration. Instead of maliciously controlling a component for an active attack, the passive attack would only passively require the attacker to monitor the network traffic on a certain location. Based on the reviewed literature, there are three common locations for monitoring and capturing in the passive attack on Tor. The following is the discussion of the three monitoring locations.

4.1. Between User and Entry OR

The attacker passively monitors network transmission between Tor's user and Entry OR. The attacker could be an ISP or anyone that could tap into the network transmission. If the attacker is located within the same local network with the user, it can correlate the Entry OR with the user's private IP address. If the attacker is on a different network, it can only correlate the user's public IP address with the Entry OR.

4.2. On Middle OR

The attacker passively monitors network transmission occur at Middle OR. It could be between Entry OR and Middle OR, or between Middle OR and Exit OR. Nevertheless, this is the least useful monitoring since both the actual sender and actual recipient of a communication message are unknown. Despite the drawbacks, it is useful for surveillance purposes [13].

4.3. Between Exit OR and Destination

The attacker passively monitors the network transmission between the Exit OR and the traffic's actual destination. An attacker that monitors this type of transmission location is commonly located close to the destination's network. The attacker only knows the destination traffic but does not know the Tor user's IP address.

5. Attack Subject in Tor Attack Studies

Table 1 classified various Tor attack studies with their corresponding attack subject. This study reviewed 80 works related to attacking the Tor platform from 2007 to 2016, within ten years. Studies that relate to Tor but not focusing on attacking Tor are excluded from this table.

Table 1 Attack studies on Tor with their corresponding attack subject

		Malicious component						**Monitoring location**			
Study	**Year**	**Entry OR**	**Middle OR**	**Exit OR**	**User**	**Destination**	**Autonomous System**	**Network Provider**	**User - Entry OR**	**Middle OR**	**Exit OR - Destination**
[14]	2007	✓		✓							
[15]	2007							✓			
[16]	2007	✓		✓							
[17]	2007						✓				
[18]	2008	✓		✓							
[19]	2008				✓						✓
[20]	2008			✓		✓					
[21]	2008							✓			
[22]	2008					✓			✓	✓	
[23]	2009	✓									
[24]	2009								✓		
[25]	2009	✓		✓							
[26]	2009			✓	✓						
[27]	2009				✓						
[28]	2009	✓		✓							
[29]	2009	✓		✓							
[30]	2009	✓		✓							
[31]	2009						✓				
[32]	2010	✓		✓							
[33]	2010			✓							
[34]	2010	✓		✓							
[35]	2011								✓		
[36]	2011	✓									
[8]	2011			✓							
[37]	2011					✓			✓		
[38]	2011				✓						
[39]	2011			✓							
[40]	2011								✓	✓	✓
[41]	2011									✓	
[42]	2011										✓
[43]	2012	✓		✓							
[44]	2012									✓	
[45]	2012									✓	
[46]	2012									✓	
[47]	2012	✓		✓							
[48]	2012		✓								
[49]	2013									✓	✓
[50]	2013									✓	
[51]	2013	✓		✓		✓					
[52]	2013				✓						
[53]	2013						✓				
[54]	2013				✓					✓	
[55]	2013	✓		✓							
[56]	2013					✓					
[57]	2014									✓	
[58]	2014									✓	
[59]	2014									✓	
[60]	2014									✓	
[61]	2014									✓	
[62]	2014									✓	
[63]	2014									✓	
[64]	2014									✓	
[65]	2014					✓				✓	
[66]	2014	✓									
[11]	2014									✓	
[9]	2014					✓				✓	
[67]	2014		✓								
[68]	2014			✓							
[69]	2015						✓				
[70]	2015						✓				
[71]	2015									✓	
[72]	2015	✓		✓							
[73]	2015						✓				
[74]	2015									✓	
[75]	2015									✓	
[76]	2015	✓								✓	
[77]	2015									✓	
[78]	2015									✓	✓
[79]	2015						✓				
[80]	2015	✓									
[81]	2015		✓								
[82]	2015									✓	
[83]	2015									✓	
[84]	2016						✓				
[12]	2016									✓	
[85]	2016									✓	
[86]	2016			✓						✓	
[87]	2016									✓	
[88]	2016									✓	
[89]	2016			✓	✓						
Total		19	3	22	7	7	8	9	29	2	5

It can be observed that the greater part of the reviewed studies focuses on passive monitoring

between user and Entry OR, followed by malicious Exit OR and Entry OR. Fig. 2 shows the attacked subject utilized in the reviewed studies throughout the years. It could be seen that between 2007 and 2014, malicious Entry OR and malicious Exit OR had been received much attention from the researchers. However, this trend had changed where starting in 2014, monitoring between user and Entry OR had received greater attention from Tor attack studies.

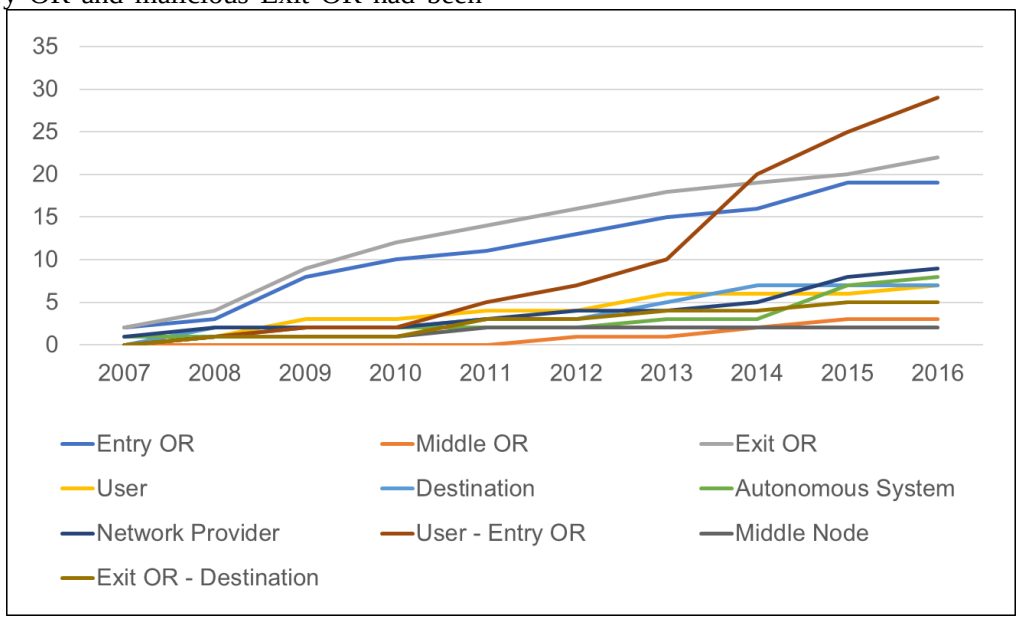

Fig. 2 Attack subject utilized in the reviewed studies throughout the years

6. Discussion

Under the presented classification, several fundamental observations could be apprehended. First, it is very important to differentiate between an attack that utilizes the active and passive technique because different attack modes require different attacking resources and preparation steps. Except for the client as a malicious component, attacking that only require traffic monitoring can be presumed as significantly easier to execute rather than controlling a malicious entity. The attacker only needs to tap the network to capture the traffic and does not require setting up any malicious component or modifying any traffic transmission. An attack that actively modifies traffic also could be detected and blocked by the Tor administrator [43, 67-68].

Despite the major differences in attacking requirements, various studies combine both actively control malicious components and, at the same time, passively monitor traffic due to these attacks partially require an actively controlled malicious component as had been carried out by [22], [37], [54], [71], [76], [86] and [9].

In addition, various studies combine both controlled Entry OR and Exit OR. Out of 19 studies that focus on controlling Entry OR, 14 also control the Exit OR simultaneously. This type of attack subject is very popular on end-to-end correlation attacks where the attacker tries to correlate traffic between the actual sender and the actual destination [43]. This kind of attack directly threatens Tor's anonymity capability, which is supposed to disassociate the communication message's actual sender and destination, which might be one reason for popularity on these active attack subjects.

Some studies could be justified as had a poor decision on the attacked subject by choosing unnecessary attack subject. The study by [23] had utilized controlled Entry OR in order to execute the attack. The authors use the Entry OR to collect traffic from Tor's users. However, this activity could be performed by passively monitoring the traffic between the user and the Entry OR. Based on how the authors use the controlled Entry OR, there is no noticeable advantage of using this high attacking resource obligation where passive monitoring could be urged as having the same capability with significantly fewer attacking resources.

As for the monitoring location, it can be observed that monitoring between user and Entry OR is the most popular passive attack subject location due to this location enables the attacker to learn the user IP address. Additionally, it could be seen that monitoring on Middle OR and monitoring between Exit OR and destination received a lack of attention from researchers. This might be because it does not provide useful information and can only be executed by ISP or autonomous system. Consequently, studies that monitoring on Middle OR does not solely use it as the attacked subject since they also utilized other means of attack subject. In an active attack, controlling the Middle OR also received a lack of focus from the researchers. However, this might still be useful compared to passive monitoring since controlling an OR will provide the attacker with cell traffic information unavailable in passive monitoring [76].

Despite the popularity of active attack subjects in Tor attack studies, the sudden popularity growth on passive monitoring between user and Entry OR since 2014 could be justified due to several potential factors. These factors include controlling malicious components become harder and easier to be detected, active attack subjects do not scale well in increasing the number of the victim, or the passive monitoring attack has become capable enough to have the same level of threat with the subject on the active attack. Howbeit, these potential factors require further in-depth exploration to be validated and substantiated. In order to do so, each of these attacks needs to be evaluated in terms of the attack procedure, the outcome of the attack, and the attack effect from an anonymity perspective. These evaluation criteria are crucial in understanding the rationale behind the changing of practice and trend among researchers on the Tor attack subject, which should be addressed in future work.

7. Conclusion

The introduction of Tor as a tool for anonymous Internet access has attracted the attention of researchers worldwide. Researchers had proposed multiple attack techniques to challenge the anonymity provided by Tor to the Internet user. In order to have a better understanding of the nature of the attack utilized in these studies, this paper has classified and analyzed these attack subjects.

The existing attack in Tor lacks in-depth investigations on the practice and trend of attack subject utilized in Tor. Despite that it is a security attack, Tor has a significantly unique subject than other security attack research fields. Each attack subject has its weaknesses and vulnerabilities that researchers relentless trying to discover. A broad investigation is carried out in this paper to understand the trend on these Tor attack subjects. Additionally, reviewing a huge number of Tor attack studies is important. It is to ensure that a wide range of possible attack scenarios is included in the analysis. If only a few studies are reviewed, the actual potential and risk of these subjects of the Tor attack might be misinterpreted or overlooked. Hence, this study provides a review and analysis of a wide range of Tor attack studies to understand better the subject these attacks utilize. This classification had yielded several new important pieces of knowledge on the practice and trend of the subject in Tor attack studies. Previously, it had been unknown that there are only three attack subjects that are popular among researchers. The other attack subjects seem to have received a lack of attention from researchers worldwide.

Hence, the knowledge obtained from this study optimistically will allow for better comprehension of the nature of the attacks executed on Tor. In addition, it will hopefully be useful for future researchers' guidance, especially in the context of practice and trends in attack subjects on Tor. Optimistically, this study should be beneficial for better comprehension of building a stronger defensive mechanism for a secure Tor environment.

Although this paper reviewed various Tor attack studies, there is a lack of in-depth investigation on each attack, especially how they utilize the attacked subject to attack Tor. A thorough understanding of the attack subject's utilization method is valuable to comprehend the practical usage of the attacked subject in Tor, where this study only discussed it briefly. This research idea should be considered for future works.

Acknowledgments

This research was supported by the Fundamental Research Grant Scheme (FRGS) of Kementerian Pendidikan Malaysia (KPM) for "Security Model: Website Fingerprinting on darknet illegal marketplaces for transaction traffic identification using machine learning" [FRGS/1/2019/ICT03/USM/02/2], School of Computer Sciences, Universiti Sains Malaysia, 11800 Pulau Pinang, Malaysia.

References

[1] SHIRAZI F., SIMEONOVSKI M., ASGHAR M. R., BACKES M., and DIAZ C. A Survey on Routing in Anonymous Communication Protocols. *Association for Computing Machinery Computing Surveys*, 2018, 51(3): 51:1-51:39. DOI:10.1145/3182658

[2] THE TOR PROJECT. Tor Metrics. 2020. Accessed December 1, 2020. https://metrics.torproject.org/

[3] SALEH S., QADIR J., and ILYAS M. U. Shedding Light on the Dark Corners of the Internet: A Survey of Tor Research. *Journal of Network and Computer Applications*, 2018, 114: 1-28. DOI: https://doi.org/10.1016/j.jnca.2018.04.002

[4] ALSABAH M. and GOLDBERG I. Performance and Security Improvements for Tor: A Survey. *Association for Computing Machinery Computing Surveys*, 2016, 49(2): 32:1-32:36. DOI:10.1145/2946802

[5] AMINUDDIN MAIM, ZAABA Z. F., SINGH M. K. M., and SINGH D. S. M. A Survey on Tor Encrypted Traffic Monitoring. *International Journal of Advanced Computer Science and Applications*, 2018, 9(8): 113-120. DOI:10.14569/IJACSA.2018.090815

[6] AMINUDDIN MAIM., ZAABA Z. F., SAMSUDIN A., JUMA'AT N. B. A, SUKARDI S., and HUSSAIN A. Classification on Deanonymisation Outcome of Tor Attack. *International Journal on Advanced Science, Engineering and Information Technology*, 2020, 29(6s): 1647-1660.

[7] JANSEN R., JUAREZ M., GÁLVEZ R., ELAHI T., and DIAZ C. Inside Job: Applying Traffic Analysis to Measure Tor from Within. In: Network and Distributed System Security Symposium (NDSS). *Internet Society*, 2018. DOI:10.14722/ndss.2018.23261

[8] CYNTHIA W., GERARD W., RADU S., ALEXANDRE D., and THOMAS E. Breaking Tor anonymity with game theory and data mining. *Concurrency and Computation Practice and Experience*, 2011, 24(10): 1052-1065. DOI:10.1002/cpe.1828

[9] ARP D., YAMAGUCHI F., RIECK K. *Torben: Deanonymizing Tor Communication Using Web Page Markers*. 2014.
[10] JOHNSON A., WACEK C., JANSEN R., SHERR M., and SYVERSON P. Users Get Routed: Traffic Correlation on Tor by Realistic Adversaries. In: *Proceedings of the 2013 Association for Computing Machinery Conference on Computer and Communications Security*, 2013: 337-348. DOI:10.1145/2508859.2516651
[11] GHAFIR I., SVOBODA J., and PRENOSIL V. Tor-based malware and Tor connection detection. In: *International Conference on Frontiers of Communications, Networks and Applications* (ICFCNA 2014 - Malaysia). ; 2014: 1-6. DOI:10.1049/cp.2014.1411
[12] SAPUTRA F. A., NADHORI I. U., and BARRY B. F. Detecting and blocking onion router traffic using deep packet inspection. In: *2016 International Electronics Symposium* (IES), 2016: 283-288. DOI:10.1109/ELECSYM.2016.7861018
[13] JAGGARD A. D. and SYVERSON P. Onions in the Crosshairs: When the Man Really is out to Get You. In: *Proceedings of the 2017 Workshop on Privacy in the Electronic Society*, 2017: 141-151. DOI:10.1145/3139550.3139553
[14] ABBOTT T. G., LAI K. J., LIEBERMAN M. R., and PRICE E. C. Browser-Based Attacks on Tor. In: BORISOV N, GOLLE P, eds. *Privacy Enhancing Technologies*. Springer Berlin Heidelberg, 2007: 184-199.
[15] YU W., FU X., GRAHAM S., XUAN D., and ZHAO W. DSSS-Based Flow Marking Technique for Invisible Traceback. In: 2007 *Institute of Electrical and Electronics Engineers Symposium on Security and Privacy*, 2007: 18-32. DOI:10.1109SP.2007.14
[16] BAUER K., MCCOY D., GRUNWALD D., KOHNO T, and SICKER D. Low-resource Routing Attacks Against Tor. In: *Proceedings of the 2007 Association for Computing Machinery Workshop on Privacy in Electronic Society*, 2007: 11-20. DOI:10.1145/1314333.1314336
[17] MURDOCH S. J. and ZIELIŃSKI P. Sampled Traffic Analysis by Internet-Exchange-Level Adversaries. In: BORISOV N., GOLLE P., eds. *Privacy Enhancing Technologies*. Springer Berlin Heidelberg, 2007: 167-183.
[18] PRIES R., YU W., FU X., and ZHAO W. A New Replay Attack against Anonymous Communication Networks. In: *2008 Institute of Electrical and Electronics Engineers International Conference on Communications*, 2008: 1578-1582. DOI:10.1109/ICC.2008.305
[19] ZANDER S., and MURDOCH S. J. An Improved Clock-skew Measurement Technique for Revealing Hidden Services. In: *17th Advanced Computing Systems Association Security Symposium (USENIX Security 08)*, 2008.
[20] CHAKRAVARTY S., STAVROU A., and KEROMYTIS A. D. Identifying Proxy Nodes in a Tor Anonymization Circuit. In: *2008 Institute of Electrical and Electronics Engineers International Conference on Signal Image Technology and Internet-Based Systems*, 2008: 633-639. DOI:10.1109/SITIS.2008.93
[21] BAI X., ZHANG Y., and NIU X. Traffic Identification of Tor and Web-Mix. In: *2008 Eighth International Conference on Intelligent Systems Design and Applications.* 1, 2008: 548-551. DOI:10.1109/ISDA.2008.209
[22] ZHANG J., DUAN H., and WU J. A Novel Method to Prevent Traffic Analysis in Low-Latency Anonymous Communication Systems. In: *2008 International Conference on Computer and Electrical Engineering*, 2008: 906-911. DOI:10.1109/ICCEE.2008.32
[23] SHI Y. and MATSUURA K. Fingerprinting Attack on the Tor Anonymity System. In: QING S., MITCHELL C. J., WANG G., eds. *Information and Communications Security*. Springer Berlin Heidelberg; 2009: 425-438. DOI:10.1007/978-3-642-11145-7_33
[24] HERRMANN D., WENDOLSKY R., and FEDERRATH H. Website Fingerprinting: Attacking Popular Privacy Enhancing Technologies with the Multinomial Naïve-Bayes Classifier. In: *Proceedings of the 2009 Association for Computing Machinery Workshop on Cloud Computing Security*, 2009: 31-42. DOI:10.1145/1655008.1655013
[25] WANG X., LUO J., YANG M., and LING Z. A novel flow multiplication attack against Tor. In: *2009 13th International Conference on Computer Supported Cooperative Work in Design*, 2009: 686-691. DOI:10.1109/CSCWD.2009.4968138
[26] EVANS N. S., DINGLEDINE R., and GROTHOFF C. A Practical Congestion Attack on Tor Using Long Paths. In: *Proceedings of the 18th Conference on the Advanced Computing Systems Association Security Symposium.* USENIX Association, 2009: 33-50. http://dl.acm.org/citation.cfm?id=1855768.1855771
[27] ZHANG Y. Effective Attacks in the Tor Authentication Protocol. In: 2009 Third International Conference on Network and System Security, 2009: 81-86. DOI:10.1109/NSS.2009.94
[28] JIN J. and WANG X. On the effectiveness of low latency anonymous network in the presence of timing attack. In: *2009 Institute of Electrical and Electronics Engineers International Conference on Dependable Systems Networks*, 2009: 429-438. DOI:10.1109/DSN.2009.5270306
[29] FU X. and LING Z. One Cell is Enough to Break Tor's Anonymity. In: *Proceedings of Black Hat Technical Security Conference*, 2009: 578-589.
[30] BAUER K., GRUNWALD D., and SICKER D. Predicting Tor path compromise by exit port. In: *2009 Institute of Electrical and Electronics Engineers 28th International Performance Computing and Communications Conference*, 2009: 384-387. DOI:10.1109/PCCC.2009.5403852
[31] EDMAN M. and SYVERSON P. AS-Awareness in Tor Path Selection. In: *Proceedings of the 16th Association for Computing Machinery Conference on Computer and Communications Security*, 2009: 380-389. DOI:10.1145/1653662.1653708
[32] JOHNSON N., MCLAUGHLIN S., and THOMPSON J. Path tracing in TOR networks. In: *18th European Signal Processing Conference*, 2010: 1856-1860.
[33] HUBER M., MULAZZANI M., and WEIPPL E. Tor HTTP Usage and Information Leakage. In: DE DECKER B., SCHAUMÜLLER I., eds. *Communications and Multimedia Security*. Springer Berlin Heidelberg, 2010: 245-255.
[34] FEIGENBAUM J., JOHNSON A., and SYVERSON P. Preventing Active Timing Attacks in Low-Latency Anonymous Communication. In: ATALLAH M. J., HOPPER N. J., eds. *Privacy Enhancing Technologies*. Springer Berlin Heidelberg, 2010: 166-183.
[35] PANCHENKO A., NIESSEN L., ZINNEN A., and ENGEL T. Website Fingerprinting in Onion Routing Based Anonymization Networks. In: *Proceedings of the 10th Annual Association for Computing Machinery Workshop on*

Privacy in the Electronic Society, 2011: 103-114. DOI:10.1145/2046556.2046570

[36] ZHANG L., LUO J., YANG M., and HE G. Application-level attack against Tor's hidden service. In: *6th International Conference on Pervasive Computing and Applications*, 2011: 509-516. DOI:10.1109/ICPCA.2011.6106555

[37] LING Z., LUO J., YU W., and FU X. Equal-Sized Cells Mean Equal-Sized Packets in Tor? In: *2011 Institute of Electrical and Electronics Engineers International Conference on Communications*, 2011: 1-6. DOI:10.1109/icc.2011.5962653

[38] ELICES J. A., PÉREZ-GONZÁLEZ F., and TRONCOSO C. Fingerprinting Tor's hidden service log files using a timing channel. In: *2011 Institute of Electrical and Electronics Engineers International Workshop on Information Forensics and Security*, 2011: 1-6. DOI:10.1109/WIFS.2011.6123154

[39] LE BLOND S, MANILS P, CHAABANE A, KÂAFAR M. A., CASTELLUCCIA C., LEGOUT A., and DABBOUS W. One Bad Apple Spoils the Bunch: Exploiting P2P Applications to Trace and Profile Tor Users. In: *Proceedings of the 4th the Advanced Computing Systems Association Conference on Large-Scale Exploits and Emergent Threats*. USENIX Association, 2011.

[40] BENMEZIANE S., BADACHE N., and BENSIMESSAOUD S. Tor Network Limits. In: 2011 *International Conference on Network Computing and Information Security*, 1, 2011: 200-205. DOI:10.1109/NCIS.2011.48

[41] BARKER J., HANNAY P., and SZEWCZYK P. Using Traffic Analysis to Identify the Second Generation Onion Router. In: *9th International Conference on Embedded and Ubiquitous Computing*, 2011: 72-78. DOI:10.1109/EUC.2011.76

[42] CHAKRAVARTY S., PORTOKALIDIS G., POLYCHRONAKIS M., and KEROMYTIS A. D. Detecting Traffic Snooping in Tor Using Decoys. In: SOMMER R., BALZAROTTI D., MAIER G., eds. *Recent Advances in Intrusion Detection*. Springer Berlin Heidelberg, 2011: 222-241.

[43] LING Z., LUO J., YU W., FU X., XUAN D, and JIA W. A New Cell-Counting-Based Attack against Tor. *Institute of Electrical and Electronics Engineers / Association for Computing Machinery Transactions on Networking*, 2012, 20(4): 1245-1261. DOI:10.1109/TNET.2011.2178036

[44] DYER K. P., COULL S. E., RISTENPART T., and SHRIMPTON T. Peek-a-Boo, I Still See You: Why Efficient Traffic Analysis Countermeasures Fail. In: *2012 Institute of Electrical and Electronics Engineers Symposium on Security and Privacy*, 2012: 332-346. DOI:10.1109/SP.2012.28

[45] CAI X., ZHANG X. C., JOSHI B., and JOHNSON R. Touching from a Distance: Website Fingerprinting Attacks and Defenses. In: *Proceedings of the 2012 Association for Computing Machinery Conference on Computer and Communications Security*, 2012: 605-616. DOI:10.1145/2382196.2382260

[46] WINTER P. and LINDSKOG S. How China Is Blocking Tor. *Computing Research Repository*. *Computer Science, Cryptography and Security*, 2012: abs/1204.0.

[47] BIRYUKOV A., PUSTOGAROV I., and WEINMANN R. P. TorScan: Tracing Long-Lived Connections and Differential Scanning Attacks. In: FORESTI S., YUNG M., MARTINELLI F., eds. *Computer Security*. Springer Berlin Heidelberg, 2012: 469-486.

[48] LING Z., LUO J., YU W., YANG M., and FU X. Extensive analysis and large-scale empirical evaluation of tor bridge discovery. In: *2012 Proceedings Institute of Electrical and Electronics Engineers INFOCOM*, 2012: 2381-2389. DOI:10.1109/INFCOM.2012.6195627

[49] SONG M., XIONG G., LI Z., PENG J., and GUO L. A de-anonymize attack method based on traffic analysis. In: *8th International Conference on Communications and Networking in China (CHINACOM)*, 2013: 455-460. DOI:10.1109/ChinaCom.2013.6694639

[50] WANG T. and GOLDBERG I. Improved Website Fingerprinting on Tor. In: *Proceedings of the 12th Association for Computing Machinery Workshop on Workshop on Privacy in the Electronic Society*, 2013: 201-212. DOI:10.1145/2517840.2517851

[51] SULAIMAN M. A. and ZHIOUA S. Attacking Tor through Unpopular Ports. In: *Institute of Electrical and Electronics Engineers 33rd International Conference on Distributed Computing Systems Workshops*, 2013: 33-38. DOI:10.1109/ICDCSW.2013.29

[52] BARBERA M. V., KEMERLIS V. P., PAPPAS V., and KEROMYTIS A. D. Cell Flood: Attacking Tor Onion Routers on the Cheap. In: CRAMPTON J., JAJODIA S., MAYES K., eds. *Computer Security*. Springer Berlin Heidelberg, 2013: 664-681.

[53] LIU P., SHI J., WANG L., WANG X., and TAN Q. IX-Level Adversaries on Entry- and Exit-Transmission Paths in Tor Network. In: *2013 Institute of Electrical and Electronics Engineers Eighth International Conference on Networking, Architecture and Storage*, 2013:1 66-172. DOI:10.1109/NAS.2013.27

[54] ELICES J. A. and PÉREZ-GONZÁLEZ F. Locating Tor hidden services through an interval-based traffic-correlation attack. In: *2013 Institute of Electrical and Electronics Engineers Conference on Communications and Network Security*, 2013: 385-386. DOI:10.1109/CNS.2013.6682740

[55] LING Z., LUO J., YU W., FU X., JIA W., and ZHAO W. Protocol-level attacks against Tor. *Computer Networks*, 2013, 57(4): 869-886. DOI:https://doi.org/10.1016/j.comnet.2012.11.005

[56] CHAN-TIN E., SHIN J., and YU J. Revisiting Circuit Clogging Attacks on Tor. In: *2013 International Conference on Availability, Reliability and Security*, 2013: 131-140. DOI:10.1109/ARES.2013.17

[57] CAI X., NITHYANAND R., WANG T., JOHNSON R., and GOLDBERG I. A Systematic Approach to Developing and Evaluating Website Fingerprinting Defenses. In: *Proceedings of the 2014 Association for Computing Machinery Conference on Computer and Communications*, 2014: 227-238. DOI:10.1145/2660267.2660362

[58] CAI X., NITHYANAND R., and JOHNSON R. CS-BuFLO: A Congestion Sensitive Website Fingerprinting Defense. In: *Proceedings of the 13th Workshop on Privacy in the Electronic Society*, 2014: 121-130. DOI:10.1145/2665943.2665949

[59] NITHYANAND R., CAI X., and JOHNSON R. Glove: A Bespoke Website Fingerprinting Defense. In: *Proceedings of the 13th Workshop on Privacy in the Electronic Society*, 2014: 131-134. DOI:10.1145/2665943.2665950

[60] JUAREZ M., AFROZ S., ACAR G., DIAZ C, and GREENSTADT R. A Critical Evaluation of Website Fingerprinting Attacks. In: *Proceedings of the 2014 Association for Computing Machinery SIGSAC Conference on Computer and Communications Security*, 2014: 263-274. DOI:10.1145/2660267.2660368

[61] HE G., YANG M., GU X., LUO J., and MA Y. A Novel Active Website Fingerprinting Attack against Tor Anonymous System. In: *Proceedings of the 2014 Institute of Electrical and Electronics Engineers 18th International Conference on Computer Supported Cooperative Work in Design*, 2014: 112-117. DOI:10.1109/CSCWD.2014.6846826

[62] SHAHBAR K. and ZINCIR-HEYWOOD AN. Benchmarking two techniques for Tor classification: Flow level and circuit level classification. In: *2014 Institute of Electrical and Electronics Engineers Symposium on Computational Intelligence in Cyber Security*, 2014: 1-8. DOI:10.1109/CICYBS.2014.7013368

[63] WANG T., CAI X., NITHYANAND R., JOHNSON R., and GOLDBERG I. Effective Attacks and Provable Defenses for Website Fingerprinting. In: *23rd Advanced Computing Systems Association Security Symposium*. USENIX Association, 2014: 143-157. https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/wang_tao

[64] HE G., YANG M., LUO J., and GU X. Inferring Application Type Information from Tor Encrypted Traffic. In: *2014 Second International Conference on Advanced Cloud and Big Data*, 2014: 220-227. DOI:10.1109/CBD.2014.37

[65] CHAKRAVARTY S., BARBERA M. V., PORTOKALIDIS G., POLYCHRONAKIS M., and KEROMYTIS A. D. On the Effectiveness of Traffic Analysis against Anonymity Networks Using Flow Records. In: FALOUTSOS M, KUZMANOVIC A, eds. *Passive and Active Measurement*. Springer International Publishing, 2014: 247-257.

[66] JANSEN R., TSCHORSCH F., JOHNSON A., and SCHEUERMANN B. The Sniper Attack: Anonymously Deanonymizing and Disabling the Tor Network. In: *Network and Distributed System Security Symposium*, 2014.

[67] SOLTANI M., NAJAFI S., and JALILI R. Mid-defense: Mitigating protocol-level attacks in TOR using indistinguishability obfuscation. In: *2014 11th International ISC Conference on Information Security and Cryptology*, 2014: 214-219. DOI:10.1109/ISCISC.2014.6994050

[68] WINTER P., KÖWER R., MULAZZANI M., HUBER M., SCHRITTWIESER S., LINDSKOG S., and WEIPPL E. Spoiled Onions: Exposing Malicious Tor Exit Relays. In: DE CRISTOFARO E., MURDOCH S.J., eds. *Privacy Enhancing Technologies*. Springer International Publishing, 2014: 304-331.

[69] HOANG N. P., ASANO Y., and YOSHIKAWA M. Anti-RAPTOR: Anti Routing Attack on Privacy for a Securer and Scalable Tor. In: *17th International Conference on Advanced Communication Technology*, 2015: 147-154. DOI:10.1109/ICACT.2015.7224775

[70] JUEN J., JOHNSON A., DAS A., BORISOV N., and CAESAR M. Defending Tor from Network Adversaries: A Case Study of Network Path Prediction. *Proceedings on Privacy Enhancing Technologies*, 2015, 2015(2): 171-187. https://content.sciendo.com/view/journals/popets/2015/2/article-p171.xml

[71] GAOFENG H., MING Y., JUNZHOU L., and XIAODAN G. A novel application classification attack against Tor. Concurrency and Computation Practice and Experience, 2015, 27(18): 5640-5661. DOI:10.1002/cpe.3593

[72] DAHAL S., LEE J., KANG J., and SHIN S. Analysis on End-to-End Node Selection Probability in Tor Network. In: *2015 International Conference on Information Networking*, 2015: 46-50. DOI:10.1109/ICOIN.2015.7057855

[73] NITHYANAND R., STAROV O., ZAIR A,. GILL P., and SCHAPIRA M. Measuring and mitigating AS-level adversaries against Tor. In: *Network and Distributed System Security Symposium 2016*, 2016. DOI:10.14722/ndss.2016.23322

[74] ALMUBAYED A., HADI A., and ATOUM J. A Model for Detecting Tor Encrypted Traffic using Supervised Machine Learning. *International Journal of Computer Network and Information Security*, 2015, 7(7): 10-23. DOI:10.5815/ijcnis.2015.07.02

[75] GU X., YANG M., and LUO J. A Novel Website Fingerprinting Attack Against Multi-Tab Browsing Behavior. In: *Institute of Electrical and Electronics Engineers 19th International Conference on Computer Supported Cooperative Work in Design*, 2015: 234-239. DOI:10.1109/CSCWD.2015.7230964

[76] KWON A., ALSABAH M., LAZAR D., DACIER M., and DEVADAS S. Circuit Fingerprinting Attacks: Passive Deanonymization of Tor Hidden Services. In: *24th Advanced Computing Systems Association Security Symposium (USENIX Security 15)*, 2015: 287-302. https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/kwon

[77] SPRINGALL A., DEVITO C., and HUANG S. H. S. Per Connection Server-Side Identification of Connections via Tor. In: *Institute of Electrical and Electronics Engineers 29th International Conference on Advanced Information Networking and Applications*, 2015: 727-734. DOI:10.1109/AINA.2015.260

[78] ISHITAKI T., ODA T., MATSUO K., BAROLLI L., and TAKIZAWA M. Performance Evaluation of a Neural Network Based Intrusion Detection System for Tor Networks Considering different Hidden Units. In: *18th International Conference on Network-Based Information Systems*, 2015: 620-627. DOI:10.1109/NBiS.2015.116

[79] SUN Y., EDMUNDSON A., VANBEVER L., LI O., REXFORD J., CHIANG M., and MITTA P. RAPTOR: Routing Attacks on Privacy in Tor. In: *24th Advanced Computing Systems Association Security Symposium (USENIX Security 15)*. 2015:271-286. https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/sun

[80] KHAN M, SADDIQUE M, PIRZADA U, ZOHAIB M., AFZAAL ALI, WADUD B., and AHMAD I. The effect of malicious nodes on Tor security. In: *2015 International Conference on Applied Research in Computer Science and Engineering*, 2015: 1-5. DOI:10.1109/ARCSE.2015.7338140

[81] LING Z., LUO J., YU W., YANG M., and FU X. Tor Bridge Discovery: Extensive Analysis and Large-scale Empirical Evaluation. *Institute of Electrical and Electronics Engineers Transactions on Parallel and Distributed Systems*, 2015, 26(7): 1887-1899. DOI:10.1109/TPDS.2013.249

[82] SHAHBAR K. and ZINCIR-HEYWOOD AN. Traffic flow analysis of Tor pluggable transports. In: *11th International Conference on Network and Service Management*, 2015: 178-181. DOI:10.1109/CNSM.2015.7367356
[83] LING Z., LUO J., WU K., YU W., and FU X. TorWard: Discovery, Blocking, and Traceback of Malicious Traffic Over Tor. *Institute of Electrical and Electronics Engineers Transactions on Information Forensics and Security*, 2015, 10(12): 2515-2530. DOI:10.1109/TIFS.2015.2465934
[84] TAN H., SHERR M., and ZHOU W. Data-plane Defenses against Routing Attacks on Tor. *Proceedings on Privacy Enhancing Technologies*, 2016, 2016(4): 276-293. https://content.sciendo.com/view/journals/popets/2016/4/article-p276.xml
[85] JAHANI H. and JALILI S. A Novel Passive Website Fingerprinting Attack on Tor Using Fast Fourier Transform. *Computer Communications*, 2016, 6: 43-51. DOI:10.1016/j.comcom.2016.05.019
[86] PANCHENKO A., LANZE F., PENNEKAMP J., ZINNEN A., HENZE M., WEHRLE K., and ENGEL T. Website Fingerprinting at Internet Scale. In: *Network and Distributed System Security Symposium*, 2016. DOI:10.14722/ndss.2016.23477
[87] WANG T. and GOLDBERG I. On Realistically Attacking Tor with Website Fingerprinting. *Proceedings on Privacy Enhancing Technologies*, 2016, 2016(4): 21-36. DOI:10.1515/popets-2016-0027
[88] HAYES J. and DANEZIS G. K-fingerprinting: A Robust Scalable Website Fingerprinting Technique. In: *25th Advanced Computing Systems Association Security Symposium (USENIX Security 16)*, 2016: 1187-1203. https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/hayes
[89] MITAKIDIS E., TAKETZIS D., FAKIS A., and KAMBOURAKIS G. SnoopyBot: An Android spyware to bridge the mixes in Tor. In*: 24th International Conference on Software, Telecommunications and Computer Networks*, 2016: 1-5. DOI:10.1109/SOFTCOM.2016.7772180

参考文:

[1] SHIRAZI F.、SIMEONOVSKI M.、ASGHAR M. R.、BACKES M. 和 DIAZ C. 匿名通信協議中的路由調查。計算機協會計算調查，2018, 51(3): 51:1-51:39。 DOI:10.1145/3182658
[2] 托 項目。 托 指標。 2020. 2020 年 12 月 1 日訪問。https://metrics.托project.org/
[3] SALEH S.、QADIR J. 和 ILYAS M. U. 揭示互聯網的黑暗角落：托 研究調查。網絡與計算機應用雜誌, 2018, 114: 1-28. DOI: https://doi.org/10.1016/j.jnca.2018.04.002
[4] ALSABAH M. 和 GOLDBERG I. 托 的性能和安全改進：一項調查。計算機協會計算調查，2016, 49(2): 32:1-32:36。 DOI:10.1145/2946802
[5] AMINUDDIN MAIM、ZAABA Z. F.、SINGH M. K. M. 和 SINGH D. S. M. 關於 托 加密流量監控的調查。國際高級計算機科學與應用雜誌, 2018, 9(8): 113-120. DOI:10.14569/IJACSA.2018.090815
[6] AMINUDDIN MAIM.、ZAABA Z. F.、SAMSUDIN A.、JUMA'AT N. B. A、SUKARDI S. 和 HUSSAIN A. 托 攻擊的去匿名化結果分類。國際先進科學、工程和信息技術雜誌，2020, 29(6s): 1647-1660。
[7] JANSEN R.、JUAREZ M.、GÁLVEZ R.、ELAHI T. 和 DIAZ C. 內部工作：應用流量分析從內部測量 托。在：網絡和分佈式系統安全研討會。互聯網協會，2018 年。DOI:10.14722/ndss.2018.23261
[8] CYNTHIA W.、GERARD W.、RADU S.、ALEXANDRE D. 和 THOMAS E. 利用博弈論和數據挖掘打破 托 匿名性。並發與計算實踐與經驗，2011, 24(10): 1052-1065。 DOI:10.1002/cpe.1828
[9] ARP D.、YAMAGUCHI F.、RIECK K. 托本：使用網頁標記對 托 通信進行去匿名化。 2014 年。
[10] JOHNSON A.、WACEK C.、JANSEN R.、SHERR M. 和 SYVERSON P. 用戶被路由：現實對手在 托 上的流量相關性。在：2013 年計算機協會計算機和通信安全會議論文集，2013：337-348。 DOI:10.1145/2508859.2516651
[11] GHAFIR I.、SVOBODA J. 和 PRENOSIL V. 基於 托 的惡意軟件和 托 連接檢測。在：國際通信、網絡和應用前沿會議。2014: 1-6。 DOI:10.1049/cp.2014.1411
[12] SAPUTRA F. A.、NADHORI I. U. 和 BARRY B. F. 使用深度數據包檢測檢測和阻止洋蔥路由器流量。在：2016 年國際電子研討會，2016 年：283-288。 DOI:10.1109/ELECSYM.2016.7861018
[13] JAGGARD A. D. 和 SYVERSON P. 十字準線中的洋蔥：當這個人真的想要抓住你的時候。在：2017 年電子社會隱私研討會論文集，2017 年：141-151。 DOI:10.1145/3139550.3139553
[14] ABBOTT T. G.、LAI K. J.、LIEBERMAN M. R. 和 PRICE E. C. 基於瀏覽器的 托 攻擊。在：BORISOV N，GOLLE P，編輯。隱私增強技術。施普林格柏林海德堡，2007：184-199。
[15] YU W.、FU X.、GRAHAM S.、XUAN D. 和 ZHAO W. 基於直接安全系統的隱形回溯流標記技術。在：2007 年電氣和電子工程師協會安全和隱私研討會，2007：18-32。 DOI:10.1109SP.2007.14
[16] BAUER K.、MCCOY D.、GRUNWALD D.、KOHNO T 和 SICKER D. 針對 托 的低資源路由攻擊。在：2007 年計算機協會電子社會隱私研討會論文集，2007：11-20。 DOI:10.1145/1314333.1314336
[17] MURDOCH S. J. 和 ZIELIŃSKI P. 互聯網交換級對手的採樣流量分析。在：BORISOV N.，GOLLE P.，編輯。隱私增強技術。施普林格柏林海德堡，2007 年：167-183。
[18] PRIES R.、YU W.、FU X. 和 ZHAO W. 一種針對匿名通信網絡的新重放攻擊。在：2008 年電氣和電子工程師學會國際通信會議，2008：1578-1582。 DOI:10.1109/ICC.2008.305

[19] ZANDER S. 和 MURDOCH S. J. 一種用於揭示隱藏服務的改進時鐘偏差測量技術。在：第 17 屆高級計算系統協會安全研討會 (USENIX 安全 08)，2008 年。
[20] CHAKRAVARTY S.、STAVROU A. 和 KEROMYTIS A. D. 在 托 匿名化電路中識別代理節點。在：2008 年電氣和電子工程師學會國際信號圖像技術和基於互聯網的系統會議，2008：633-639。 DOI:10.1109/SITIS.2008.93
[21] BAI X.，ZHANG Y.，和 NIU X. 托 和網絡混合的流量識別。在：2008 年第八屆智能係統設計與應用國際會議。 2008 年 1 月：548-551。 DOI:10.1109/ISDA.2008.209
[22] ZHANG J.，DUAN H.，和 WU J. 一種防止低延遲匿名通信系統流量分析的新方法。在：2008 年計算機與電氣工程國際會議，2008：906-911。 DOI:10.1109/ICCEE.2008.32
[23] SHI Y. 和 MATSUURA K. 對 托 匿名系統的指紋攻擊。在：QING S.，MITCHELL C. J.，WANG G.，編輯。信息和通信安全。施普林格柏林海德堡； 2009 年：425-438。 DOI:10.1007/978-3-642-11145-7_33
[24] HERRMANN D.、WENDOLSKY R. 和 FEDERRATH H. 網站指紋識別：使用多項樸素貝葉斯分類器攻擊流行的隱私增強技術。在：2009 年計算機協會雲計算安全研討會論文集，2009 年：31-42。 DOI:10.1145/1655008.1655013
[25] WANG X.，LUO J.，YANG M.，和 LING Z. 一種針對 托 的新型流量乘法攻擊。在：2009 年第 13 屆計算機支持設計協同工作國際會議，2009：686-691。 DOI:10.1109/CSCWD.2009.4968138
[26] EVANS N. S.、DINGLEDINE R. 和 GROTHOFF C. 使用長路徑對 托 進行實際擁塞攻擊。在：高級計算系統協會安全研討會第 18 屆會議論文集。USENIX 協會，2009 年：33-50。 http://dl.acm.org/citation.cfm?id=1855768.1855771
[27] 張 Y. 托 身份驗證協議中的有效攻擊。見：2009 第三屆網絡與系統安全國際會議，2009：81-86。 DOI:10.1109/NSS.2009.94
[28] JIN J. 和 WANG X. 存在定时攻击的低延迟匿名网络的有效性。在：2009 年電氣和電子工程師學會可靠系統網絡國際會議，2009：429-438。 DOI:10.1109/DSN.2009.5270306
[29] FU X. 和 LING Z. 一個細胞足以打破 托 的匿名性。在：黑帽技術安全會議論文集，2009 年：578-589。
[30] BAUER K.、GRUNWALD D. 和 SICKER D. 通過出口端口預測 托 路徑妥協。在：2009 電氣和電子工程師學會第 28 屆國際性能計算和通信會議，2009：384-387。 DOI:10.1109/PCCC.2009.5403852
[31] EDMAN M. 和 SYVERSON P. 意識在托 路徑選擇。在：第 16 屆計算機協會計算機和通信安全會議論文集，2009：380-389。 DOI:10.1145/1653662.1653708
[32] JOHNSON N.、MCLAUGHLIN S. 和 THOMPSON J. 托 網絡中的路徑追踪。在：第 18 屆歐洲信號處理會議，2010：1856-1860。
[33] HUBER M.、MULAZZANI M. 和 WEIPPL E. 托 HTTP 使用和信息洩漏。在：DE DECKER B.，SCHAUMÜLLER I.，編輯。通信和多媒體安全。施普林格柏林海德堡，2010 年：245-255。
[34] FEIGENBAUM J.、JOHNSON A. 和 SYVERSON P. 防止低延遲匿名通信中的主動定時攻擊。在：ATALLAH M. J.，HOPPER N. J.，編輯。隱私增強技術。施普林格柏林海德堡，2010 年：166-183。
[35] PANCHENKO A.、NIESSEN L.、ZINNEN A. 和 ENGEL T. 基於洋蔥路由的匿名網絡中的網站指紋識別。在：第 10 屆計算機協會年度協會電子社會隱私研討會論文集，2011：103-114。 DOI:10.1145/2046556.2046570
[36] 張 L.，LUO J.，YANG M.，和 HE G. 針對 托 隱藏服務的應用級攻擊。在：第六屆普及計算和應用國際會議，2011：509-516。 DOI:10.1109/ICPCA.2011.6106555
[37] LING Z.，LUO J.，YU W.，和 FU X. 在 托 中，相同大小的單元是否意味著相同大小的數據包？在：2011 年電氣與電子工程師學會國際通信會議，2011：1-6。 DOI:10.1109/icc.2011.5962653
[38] ELICES J. A.、PÉREZ-GONZÁLEZ F. 和 TRONCOSO C. 使用定時通道對 托 的隱藏服務日誌文件進行指紋識別。在：2011 年電氣和電子工程師協會國際信息取證和安全研討會，2011：1-6。 DOI:10.1109/WIFS.2011.6123154
[39] LE BLOND S、MANILS P、CHAABANE A、KÂAFAR M. A.、CASTELLUCCIA C.、LEGOUT A. 和 DABBOUS W。一個壞蘋果破壞了一群人：利用点对点應用程序來跟踪和分析 托 用戶。在：關於大規模漏洞利用和緊急威脅的第四屆高級計算系統協會會議的論文集。USENIX 協會，2011 年。
[40] BENMEZIANE S.、BADACHE N. 和 BENSIMESSAOUD S. 托 網絡限制。在：2011年網絡計算與信息安全國際會議，1，2011：200-205。 DOI:10.1109/NCIS.2011.48
[41] BARKER J.、HANNAY P. 和 SZEWCZYK P. 使用流量分析來識別第二代洋蔥路由器。在：第 9 屆嵌入式和無處不在計算國際會議，2011：72-78。 DOI:10.1109/EUC.2011.76
[42] CHAKRAVARTY S.、PORTOKALIDIS G.、POLYCHRONAKIS M. 和 KEROMYTIS A. D. 使用誘餌檢測 托 中的流量窺探。在：SOMMER R.，BALZAROTTI D.，MAIER G.，編輯。入侵檢測的最新進展。施普林格柏林海德堡，2011：222-241。
[43] LING Z.、LUO J.、YU W.、FU X.、XUAN D 和 JIA W. 一種基於細胞計數的新型 托

攻擊。電氣和電子工程師協會/計算機協會網絡交易，20 12, 20(4): 1245-1261。 DOI:10.1109/TNET.2011.2178036
[44] DYER K. P.、COULL S. E.、RISTENPART T. 和 SHRIMPTON T. 躲貓貓，我仍然看到你：為什麼有效的交通分析對策失敗。在：2012
年電氣和電子工程師協會安全和隱私研討會，2012：332 -346。 DOI:10.1109/SP.2012.28
[45] CAI X.、ZHANG X. C.、JOSHI B. 和 JOHNSON R. 遠距離觸摸：網站指紋攻擊和防禦。在：2012
年計算機協會計算機和通信安全會議論文集，2012：605 -616。 DOI:10.1145/2382196.2382260
[46] WINTER P. 和 LINDSKOG S. 中國如何阻止托。計算研究資料庫。計算機科學、密碼學和安全，201 2 年：abs/1204.0。
[47] BIRYUKOV A.、PUSTOGAROV I. 和 WEINMANN R. P. 托扫描：跟踪長期連接和差分掃描攻擊。在：FORESTI S.，YUNG M.，MARTINELLI F.，編輯。計算機安全。施普林格柏林海德堡， 2012: 469-486。
[48] LING Z.，LUO J.，YU W.，YANG M.，和 Fu X. 托橋發現的廣泛分析和大規模實證評估。在：2012
年會刊電氣和電子工程師協會信息通信， 2012: 2381-2389。 DOI:10.1109/INFCOM.2012.6195627
[49] SONG M.，XIONG G.，LI Z.，PENG J.，和 GUO L. 基於流量分析的去匿名化攻擊方法。在：第八屆中國通信與網絡國際會議（中國通信）， 2013: 455-460. DOI:10.1109/ChinaCom.2013.6694639
[50] WANG T. 和 GOLDBERG I. 改進 托上的網站指紋識別。在：計算機協會第 12 屆電子社會隱私研討會議論文集，2013：201-212。 DOI:10.1145/2517840.2517851
[51] SULAIMAN M. A. 和 ZHIOUA S. 通過不受歡迎的端口攻擊
托。在：電氣和電子工程師學會第 33 屆分佈式計算系統研討會國際會議，2013 年：33-38。 DOI:10.1109/ICDCSW.2013.29
[52] BARBERA M. V.、KEMERLIS V. P.、PAPPAS V. 和 KEROMYTIS A. D. 细胞泛濫：廉價攻擊 托洋蔥路由器。在：CRAMPTON J.，JAJODIA S.，MAYES K.，編輯。計算機安全。施普林格柏林海德堡，2013: 664-681。
[53] LIU P.，SHI J.，WANG L.，WANG X.，和 TAN Q. 托網絡中進入和退出傳輸路徑的 IX 級對手。在：2013 年電氣和電子工程師協會第八屆網絡、架構和存儲國際會議，2013：1 66-172。 DOI:10.1109/NAS.2013.27
[54] ELICES J. A. 和 PÉREZ-GONZÁLEZ F. 通過基於間隔的流量相關性攻擊定位 托隱藏服務。在：2013
年電氣和電子工程師學會通信與網絡安全會議，2013：3 85-386。 DOI:10.1109/CNS.2013.6682740
[55] LING Z.、LUO J.、YU W.、FU X.、JIA W. 和 ZHAO W. 針對 托 的協議級攻擊。計算機網絡，2013, 57(4): 869-886。DOI: https://DOI.org/10.1016/j.comnet.2012.11.005
[56] CHAN-TIN E.、SHIN J. 和 YU J. 重溫 托上的電路阻塞攻擊。在：2013
年可用性、可靠性和安全性國際會議，2013 年：131-140。 DOI:10.1109/ARES.2013.17
[57] CAI X.、NITHYANAND R.、WANG T.、JOHNSON R. 和 GOLDBERG I. 開發和評估網站指紋防禦的系統方法。在：2014
年計算機協會計算機和通信會議論文集，2014：227-238。 DOI:10.1145/2660267.2660362
[58] CAI X.、NITHYANAND R. 和 JOHNSON R. CS-布法羅：擁塞敏感網站指紋防禦。在：第 13 屆電子社會隱私研討會論文集，2014 年：121-130。 DOI:10.1145/2665943.2665949
[59] NITHYANAND R.、CAI X. 和 JOHNSON R. 手套：定制的網站指紋防禦。在：第 13 屆電子社會隱私研討會論文集，2014 年：131-134。 DOI:10.1145/2665943.2665950
[60] JUAREZ M.、AFROZ S.、ACAR G.、DIAZ C 和 GREENSTAT R. 對網站指紋攻擊的批判性評估。在：2014
年計算機協會計算機和通信安全會議論文集，2014：263 -274。 DOI:10.1145/2660267.2660368
[61] HE G.，YANG M.，GU X.，LUO J.，和 MA Y. 一種針對托匿名系統的新型主動網站指紋攻擊。在：201 4 年電氣和電子工程師學會第 18 屆計算機支持設計合作工作國際會議論文集，2014：112 -117。 DOI:10.1109/CSCWD.2014.6846826
[62] SHAHBAR K. 和 ZINCIR-HEYWOOD AN。對 托分類的兩種技術進行基準測試：流量級別和電路級別分類。在：2014
電氣和電子工程師協會網絡安全計算智能研討會，2014 ：1-8。 DOI:10.1109/CICYBS.2014.7013368
[63] WANG T.、CAI X.、NITHYANAND R.、JOHNSON R. 和 GOLDBERG I. 網站指紋識別的有效攻擊和可證明防禦。在：第 23 屆高級計算系統協會安全研討會。 USENIX 協會，2014：143-157。
https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/wang_tao
[64] HE G.，YANG M.，LUO J.，和 GU X. 從託加密流量推斷應用程序類型信息。在：2014
年第二屆高級雲和大數據國際會議，2014：220-227。 DOI:10.1109/CBD.2014.37
[65] CHAKRAVARTY S.、BARBERA M. V.、PORTOKALIDIS G.、POLYCHRONAKIS M. 和 KEROMYTIS A. D. 關於使用流記錄對匿名網絡進行流量分析的有效性。在：FALOUTSOS M, KUZMANOVIC A,編輯。被動和主動測量。施普林格國際出版社，2014 年：247-257。
[66] JANSEN R.、TSCHORSCH F.、JOHNSON A. 和 SCHEUERMANN B. 狙擊手攻擊：匿名去匿名化和禁用托 網絡。在：網絡和分佈式系統安全研討會，2014 年。
[67] SOLTANI M.、NAJAFI S. 和 JALILI R. 中防：使用不可區分性混淆緩解 托中的協議級攻擊。在：2014 年第 11

届信息安全和密碼學國際国际学习中心會議，2014：214-219。 DOI:10.1109/ISCISC.2014.6994050

[68] WINTER P.、KÖWER R.、MULAZZANI M.、HUBER M.、SCHRITTWIESER S.、LINDSKOG S. 和 WEIPPL E. 被寵壞的洋蔥：暴露惡意 托 出口繼電器。在：DE CRISTOFARO E., MURDOCH S.J., 編輯。隱私增強技術。施普林格國際出版社，2014 年：304-331。

[69] HOANG N. P.、ASANO Y. 和 YOSHIKAWA M. 反猛禽：針對安全和可擴展 托 的隱私反路由攻擊。在：第 17 屆先進通信技術國際會議，2015：147-154。 DOI:10.1109/ICACT.2015.7224775

[70] JUEN J.、JOHNSON A.、DAS A.、BORISOV N. 和 CAESAR M. 防禦網絡對手的 托：網絡路徑預測的案例研究。隱私增強技術論文集，2015，2015(2)：171-187。 https://content.sciendo.com/view/journals/popets/2015/2/article-p171.xml

[71] GAOFENG H., MING Y., JUNZHOU L., 和 XIAODAN G. 一種針對 托 的新型應用程序分類攻擊。並發與計算實踐與經驗, 2015, 27(18): 5640-5661. DOI:10.1002/cpe.3593

[72] DAHAL S.、LEE J.、KANG J. 和 SHIN S. 托 網絡中端到端節點選擇概率的分析。在：2015 年國際信息網絡會議，2015：46-50。 DOI:10.1109/ICOIN.2015.7057855

[73] NITHYANAND R., STAROV O., ZAIR A,. GILL P. 和 SCHAPIRA M. 衡量和減輕針對 托 的作為級對手。在：2016 年網絡和分佈式系統安全研討會，2016 年。DOI:10.14722/ndss.2016.23322

[74] ALMUBAYED A.、HADI A. 和 ATOUM J. 使用監督機器學習檢測 托 加密流量的模型。國際計算機網絡與信息安全學報, 2015, 7(7): 10-23. DOI:10.5815/ijcnis.2015.07.02

[75] GU X.、YANG M. 和 LUO J. 一種針對多標籤瀏覽行為的新型網站指紋攻擊。在：電氣和電子工程師學會第 19 屆計算機支持設計協同工作國際會議，2015：234-239。 DOI:10.1109/CSCWD.2015.7230964

[76] KWON A.、ALSABAH M.、LAZAR D.、DACIER M. 和 DEVADAS S. 電路指紋攻擊：托 隱藏服務的被動去匿名化。在：第 24 屆高級計算系統協會安全研討會（USENIX 安全 15），2015：287-302。 https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/kwon

[77] SPRINGALL A.、DEVITO C. 和 HUANG S. H. S. 每個連接服務器端的連接標識通過托。在：電氣和電子工程師學會第 29 屆高級信息網絡與應用國際會議，2015：727-734。 DOI:10.1109/AINA.2015.260

[78] ISHITAKI T.、ODA T.、MATSUO K.、BAROLLI L. 和 TAKIZAWA M. 考慮不同隱藏單元的 托 網絡的基於神經網絡的入侵檢測系統的性能評估。在：第 18 屆基於網絡的信息系統國際會議，2015：620-627。 DOI:10.1109/NBiS.2015.116

[79] SUN Y.、EDMUNDSON A.、VANBEVER L.、LI O.、REXFORD J.、CHIANG M. 和 MITTA P. RAP托：對 托 中隱私的路由攻擊。在：第 24 屆高級計算系統協會安全研討會 (USENIX 安全 15)。2015:271-286。 https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/sun

[80] KHAN M、SADDIQUE M、PIRZADA U、ZOHAIB M.、AFZAAL ALI、WADUD B. 和 AHMAD I。惡意節點對 托 安全的影響。在：2015年計算機科學與工程應用研究國際會議，2015年：1-5。 DOI:10.1109/ARCSE.2015.7338140

[81] LING Z.、LUO J.、YU W.、YANG M. 和 FU X. 托橋樑發現：廣泛分析和大規模實證評估。電氣與電子工程師學會並行與分佈式系統彙刊，2015，26(7)：1887-1899。 DOI:10.1109/TPDS.2013.249

[82] SHAHBAR K. 和 ZINCIR-HEYWOOD AN。 托 可插拔傳輸的流量分析。在：第 11 屆網絡和服務管理國際會議，2015：178-181。DOI:10.1109/CNSM.2015.7367356

[83] LING Z.、LUO J.、WU K.、YU W. 和 FU X. 托病房：托 上惡意流量的發現、阻止和追溯。電氣與電子工程師學會信息取證與安全彙刊，2015，10(12)：2515-2530。 DOI:10.1109/TIFS.2015.2465934

[84] TAN H.、SHERR M. 和 ZHOU W. 數據平面防御路由攻擊托。隱私增強技術論文集，2016，2016(4)：276-293。 https://content.sciendo.com/view/journals/popets/2016/4/article-p276.xml

[85] JAHANI H. 和 JALILI S. 使用快速傅立葉變換對 托 進行新型被動網站指紋攻擊。計算機通信，2016，6：43-51。 DOI:10.1016/j.comcom.2016.05.019

[86] PANCHENKO A.、LANZE F.、PENNEKAMP J.、ZINNEN A.、HENZE M.、WEHRLE K. 和 ENGEL T. 互聯網規模的網站指紋識別。在：網絡和分佈式系統安全研討會，2016. DOI:10.14722/ndss.2016.23477

[87] WANG T. 和 GOLDBERG I. 關於用網站指紋實際攻擊 托。隱私增強技術論文集，2016，2016(4)：21-36。 DOI: 10.1515/popets-2016-0027

[88] HAYES J. 和 DANEZIS G. K-指紋：一種強大的可擴展網站指紋技術。在：第 25 屆高級計算系統協會安全研討會（USENIX 安全16），2016：1187-1203。 https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/hayes

[89] MITAKIDIS E.、TAKETZIS D.、FAKIS A. 和 KAMBOURAKIS G. 史努比機器人：一種安卓間諜軟件，用於連接 托 中的混合。在：第 24 屆軟件、電信和計算機網絡國際會議，2016：1-5。 DOI:10.1109/SOFTCOM.2016.7772180