IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-6, Issue-10, Oct 2018 E-ISSN: 2347-2693

Study Report of existing forensic tools and technologies to identify Darknet

Preeti S. Joshi[1*] and Dinesha H.A.[2]

[1] Department of Information Technology, Marathwada MitraMandal's College of Engineering, SPPU, Pune, India
[2] Department of Computer Science and Engineering, Jain College of Engineering, VTU, Belagavi, India

[*]*Corresponding Author: preetijoshi@mmcoe.edu.in, Tel.: +91-922552-4663*

Available online at: www.ijcseonline.org

Accepted: 30/Sept/2018, Published: 31/Oct/2018

***Abstract*—** DarkNet is the portion of Internet that is intentionally kept hidden and is only accessible by special soft wares and non-standard communication protocols and ports. Accessing these portion is not illegal at all times, but these software make it possible to keep the user anonymous and preserve data privacy. Anonymous communication has gained popularity and is of much interest. Anonymity leads to compromising nonrepudiation and security goals. Apart from providing freedom of speech to user, anonymity also provides conducive environment to illegal activities and different kinds of cyber-attacks. Network surveillance and forensic investigation is required to reconstruct or collect evidence but becomes a challenge due to anonymity, encryption and newer ways of cyber-attack. Innovative methods and techniques are required for overcoming these challenges of DarkNet. Sniffing the network for information, traffic analysis, anomaly and intrusion detection are few techniques to find evidences. With a plethora of tools and techniques available for collecting, identifying, processing and analyzing data on the networks, we try to explore few tools for forensic investigation in the DarkNet.

***Keywords*—** *Darknet, Freenet, I2P, Tor, whonix*

I. INTRODUCTION

Data that we search using typical search engines like Google, Bing, Yahoo etc. is called the surface web or clear web and is just 4% of the entire web content. A part of the web which is not indexed by these search engines is called Deep web. Contents in Deep Web are stored in databases or are accessible through the links on the website making it unsearchable by search engines. So they are said to be deep in the Web. DarkNet or DarkWeb covers all the websites and hidden services which is intentionally kept hidden by encryption and obfuscation and needs special software to access them [1]. Popular tools like Tor, Freenet, I2P provides anonymity and to access DarkNet and are used by, criminals to access illegal sites for drug sale, child pornography, weapons etc. Threats like Cryptolocker ransomware or the CTB locker have picked up and uses anonymous communication systems like Tor [2]. DarkNets are also used by whistleblowers, journalist, activist and bloggers to avoid censorship. Forensic investigation in DarkNet aims at Capturing/Monitor the traffic over the network and analyse the traffic to identify traffic pattern or signature of an attack, identifying user behaviour etc. Challenges faced by these activities due to inherent nature DarkNet are to overcome encryption, anonymity, dynamic nature of websites etc. The scope of the paper is to review the techniques providing anonymity for accessing the DarkNet and compare the tools for forensic investigation in DarkNet. Section II presents the techniques of accessing the DarkNet. Section III compares tools for packet sniffing, protocol analysers, intrusion detection systems and visualization and monitoring.

II. STAYING ANONYMOUS

A virtual private network creates a tunnel for data transmitted for privacy and security. VPN thus provides anonymous browsing over internet. This is a limited form of anonymity as the service provider of the VPN knows what the user is doing and his location. Various technologies like tor, Freenet, I2P and operating system like whonix provide anonymous browsing and are required for accessing the DarkNet sites or the onion services also called as hidden services.

In the paper [3] the author describes the anonymous communication systems Tor, I2P, JAP, Tarzan, Morphix, Mute, Free net. Tor and I2P are compared thoroughly concluding that that Tor has benefits over I2P. While in [4] the author compares the anonymity, reliability, cost and performance of tools namely tor, I2P and JonDonym with respect to Round Trip Time (RTT), Inter Packet Delay Variance (IPDV) and throughput.

Tor-The Onion Router - Tor provides anonymous browsing on the internet by hiding identity of source and destination. The obfuscation of network traffic through intermediate nodes called relays is made possible by distributing transaction over several places on the internet. Thus a circuit is built, where each node knows only the previous and next node in the circuit and a separate encryption key for each hop [5].

Freenet- Freenet is a distributed P2P platform that permits the publication, replication, and retrieval of data and provides anonymity to user. Each node provides storage and helps in routing request. Files to be stored are divided into pieces, with each piece stored at a different node. On request these are reassembled downloaded for the user. It works similar to Tor's hidden services and stores previously added files in freenet. It is more of a datastore. The request for data is randomly routed through nodes in the freenet. Users uploading and downloading files are hidden [6].

I2P- Invisible Internet Project - I2P is an anonymous overlay network. To anonymize the messages sent, each client application has their I2P "router" to build inbound and outbound "tunnels" - a sequence of peers that pass messages in one direction to and from the client, respectively. In turn, when a client wants to send a message to another client, the client passes that message out one of their outbound tunnels targeting one of the other client's inbound tunnels, eventually reaching the destination. Every participant in the network chooses the length of these tunnels, and in doing so, makes a trade-off between anonymity, latency, and throughput according to their own needs. I2P uses a variation of onion routing called garlic routing in which several messages along with their delivery instructions can be encapsulated into a single message and encrypted with the receiver's key [7].

Whonix- Whonix is a desktop operating system designed for advanced security and privacy. Whonix mitigates the threat of common attack vectors while maintaining usability. Online anonymity is realized via fail-safe, automatic, and desktop-wide use of the Tor network. A heavily reconfigured Debian base is run inside multiple virtual machines, providing a substantial layer of protection from malware and IP address leaks. Commonly used applications are pre-installed and safely pre-configured for immediate use. The user is not jeopardized by installing additional applications or personalizing the desktop. Whonix is under active development and is the only operating system designed to be run inside a VM and paired with Tor [8].

III. TOOLS

A. Packet Capture/Sniffing

The first and foremost task in any kind of digital forensic activity is to collect evidence. This can be accomplished by packet sniffing tools that intercept data flowing on the network. Table I lists few of the sniffing tools and compares them with respect to platform they run and their capability in sniffing. Tcpdump, fiddler freely available of which Tcpdump is a command line tool that sniffs the network. There are other tools like dsniff, filesnarf and mailsnarf that sniffs passwords, files and mails respectively. Network miner is also free and can extract files, emails and certificates transferred over the network

B. Protocol Analyser

A protocol Analyser captures as well as analyses the data flowing in the network. The task of protocol analyser is to assess network performance, application performance and security. These tools capture as well as analyse the network traffic. It can be either online or it can work offline on the data captured and stored previously. Table I lists few protocol analysers and compares them with respect to their capability. Fiddler and Network miner are freely available but the most popular freely available tool wireshark previously known as ethereal captures 1100 protocols, whereas capsa is a product sold by Colasoft.

TABLE I. LIST OF FEW PACKET SNIFFER & PROTOCOL ANALYSER

Tool	Platform	Category	Working
Tcpdump Windump	Linux Windows	Sniffer	Limited protocol decoding
Fiddler[9]	Linux,Windows Mac, Solaris, ioS, Android	Sniffer	Used for HTTP investigation
Network Miner [10]	Windows, Linux, Mac	Sniffer/ Visualization tool	To reconstruct files that were sent over the network.
Wireshark/tshark[11]	Windows, Linux, macOS, Solaris, FreeBSD, etc.	Protocol Analyser	Deep Inspection of hundreds of protocol
Capsa[12]	Windows	Protocol Analyser	In-depth packet decoding
Netsniff-ng[13]	Linux	Network Analyser	A zero-copy analyzer

C. Network Intrusion Detection System

A network intrusion detection system (IDS) is a device or software that monitors network traffic and issues an alert if suspicious activity is detected. Whereas an intrusion Prevention system (IPS) reacts to malicious activity by rejecting or dropping the data packets on the network. Thus preventing cyber-attacks. An IDS is categorised as host based also called HIDS, if it monitors a single system or host and network based, NIDS if it monitors a network. For intrusion detection. IDS are also categorised based on the method of detection as signature based intrusion detection system if it

works depending on rules or signatures of intrusion and anomaly based intrusion detection system if it works by searching for anomaly in network traffic. Table II lists few IDS systems and compares them with respect to the platform, method of working and mode of operation. Out of given IDS, Snort and suricata are rule based, suricata however is also multithreaded and can work with large volumes. Bro is both signature based and anomaly based IDS. Security onion is enterprise monitoring tool and includes snort, kibana [21], suricata etc.

TABLE II. LIST OF FEW INTRUSION DETECTION SYSTEM

IDS	Open Source/ Commercial	Method	Platform	Mode
Snort [14]	FOSS	Sniffer, packet logger, NIDS content searching and matching	Linux, Windows	For Real time detection
Suricata [15]	FOSS	NIDS,IPS	Windows, **Linux** /Unix, and Mac	Inline IPS & offline PCAP
Bro IDS [16]	FOSS	Network traffic analyzer + IDS	Linux, FreeBSD, and MacOS	Online & offline
Security Onion [17]	FOSS	HIDS,NIDS security monitor, logger	Linux based	Real time
OpenWIPS-NG [18]	FOSS	IPS (For Wireless Network)	Linux	Real time
Kismet [19]	Open source	Sniffer, IDS (For Wireless Network)	Linux, Windows	Real time
NetDetector [20]	Commercial Software	Packet capture, IDS, Reconstructing Network activity	Windows	Real Time

D. Visualization and Monitoring tools

Data captured by packet sniffer and analysed by protocol analyser need further investigation and tools to report the findings by visuals.

NetViewer is a free release to the general public as a visualization tool. NetViewer can provide information on traffic distributions over IP address/port number domains, utilization of link capacity and effectiveness of Quality of Service policies. It is also employed to detect and identify network anomalies such as DoS/DDoS attacks, worms. NetViewer consists of five major software components: the packet parser, the signal computing engine, the detection engine, the visualization engine and the alerting engine [21].

Netflow is a network monitoring tool to monitor network bandwidth and traffic patterns at an interface-specific level. It also tracks network anomalies that surpass network firewall, identifies context-sensitive anomalies and zero-day intrusions and monitors application specific usage [22].

Kibana is an open source data visualization plugin for Elasticsearch. It provides visualization capabilities on top of the content indexed on an Elasticsearch cluster. Users can create bar, line and scatter plots, or pie charts and maps on top of large volumes of data [23].

IV. CONCLUSION

A large part of internet traffic is over DarkNet, where most of the activities are result of attack, errors and are not legal or the motive is to avoid censorship. This is conceivable by techniques providing anonymity and privacy like Tor, Freenet, I2P, whonix etc. Using these techniques to access the web is not illegal and so cannot be banned. In the presence of both traffic of surface web or opennet and that of DarkNet, evidences of illegal digital activities are often suppressed in huge volumes of data. It becomes difficult to search to detect crimes and collect evidence. Tools like packet sniffers, protocol analyzer, intrusion detection systems and tools for visualization of this network data can provide support for forensic investigation to some extent. Innovative techniques are required to overcome the hurdles of anonymity and encryption. The weakness of the anonymous communication system if identified can provide some insight into the traffic analysis and monitoring. Thus anonymous traffic over DarkNet has tremendous scope for research and analysis.

ACKNOWLDGMENT

Our sincere thanks to Dr. K.G. Vishwanath, Principal and Director, CSE Research centre head, Jain College if Engineering, Belagavi, and Dr. S.M. Deshpande, Principal, Marathwada MitraMandal's College of Engineering, Pune and Dr. V.S. Bidve, HOD IT Marathwada Mitramandal's college of Engineering, Pune for the encouragement.

REFERENCES

[1] Dr. Digvijaysinh Rathod," Darknet forensic", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 6, Issue 4, July- August 2017

[2] Rhyme Upadhyaya, Aruna Jain, "Cyber Ethics and Cyber Crime: a deep dwelved study into legality, ransomware, underground web and bitcoin wallet ", Published in International Conference on Computing, Communication and Automation (ICCCA), pp.143-148 ,2016

[3] Afzaal Ali, Maria Khan, Muhammad Saddique , Umar Pirzada, Muhammad Zohaib, Imran Ahmad, Narayan Debnath " TOR vs I2P: A Comparative Study", Published in: 2016 IEEE International Conference on Industrial Technology (ICIT), pp.1748-1751, 2016

[4] Thorsten Ries, Andriy Panchenko, Radu State and Thomas Engel , "Comparison of Low-Latency Anonymous Communication Systems - Practical Usage and Performance", AISC '11 Proceedings of the Ninth Australasian Information Security Conference - Volume 116, 2011
[5] Roger Dingledine, Nick Mathewson, Paul Syverson," Tor: The Second-Generation Onion Router", 13th conference on USENIX Security Symposium - Volume 13, 2004
[6] Clarke I., Sandberg O., Wiley B., Hong T.W. (2001) Freenet: A Distributed Anonymous Information Storage and Retrieval System. In: Federrath H. (eds) Designing Privacy Enhancing Technologies. Lecture Notes in Computer Science, vol 2009. Springer, Berlin, Heidelberg.
[7] Juan Pablo Timpanaro, Isabelle Chrisment, and Olivier Festor, "A Bird's Eye View on the I2P Anonymous File-sharing Environment", Proceedings of the 6th International Conference on Network and System Security, pp.135-148, 2012.
[8] Whonix, www.whonix.org/wiki, 25-Aug- 2018
[9] Packet Sniffer-Fiddler, https://www.telerik.com/fiddle, 25-Aug- 2018
[10] Netminer Sniffer and Network Visualization tool, www.netminer.com, 25-Aug- 2018
[11] Wireshark and ethereal network protocol analyser toolkit,1st edition, elsevier,ISBN: 9781597490733
[12] Capsa Real time portable network anlalyser, Users Guide, 2018
[13] Netsnigg-ng as Network analyser, www.netsniff-ng.org, 20-Sep 2018
[14] M Roesch - Lisa , " Snort: lightweight intrusion detection network", Proceedings of LISA '99: 13th Systems Administration Conference, 1999
[15] Suricata IDS, www.suricata-ids.org, 25-Aug- 2018
[16] Bro IDS, www.bro.org/sphinx/intro, 25-Aug - 2018
[17] Security Onion IDS, www.securityonion.net, 25-Aug - 2018
[18] Openwips IPS, www.openwips-ng.org, 25-Aug - 2018
[19] Kismet IDS, www.kismetwireless.net/ 25-Aug - 2018
[20] NetDetecor IDS, www.niksun.com, 25-Aug - 2018
[21] Seong Soo Kim and A. L. Narasimha Reddy, "NetViewer: A Network Traffic Visualization and Analysis Tool" Texas A&M University, 19th Large Installation System Administration Conference (LISA '05), 2005
[22] Network monitoring tool, www.manageengine.com/products/netflow, 25-Aug - 2018
[23] Elasticsearch, www.elastic.co/products/kibana 25-Aug - 2018

Authors Profile

Mrs. Preeti. S. Joshi pursued Bachelor of computer Science from Shivaji University,Kolhapur, Maharashtra, India in 1999 and M.E in Information Technology from Mumbai University, India in 2007. She is currently working as Assistant Professor in Department of Information Technology at Marathwada MitraMandal's College of Engineering,Pune, India. She has 15 years of teaching experience .

Dinesha H.A. pursued Bachelor of Science from Malnad College of Engineering, Hassan, Karnataka, India, in 2007 and M.Tech in software Enginering from R.V. College of Engineering Bengaluru, Karnataka, India in 2009. He pursued Ph.D. from VTU, Belagavi, Karnataka, India in 2017 and is currently working as Associate proffessor at Jain College of Engineering, Belagavi, Karnataka, India. He has several research papers in reputed international journals and conferences including IEEE and it's also available online. His main research work focuses on colud computing. He has 8 years of teaching experience and 2 years of Research Experience.

