LUPINE PUBLISHERS

Advances in Robotics & Mechanical Engineering

DOI: 10.32474/ARME.2021.03.000157

ISSN: 2643-6736

Research Article

Avoiding Vulnerabilities and Attacks with a Proactive Strategy for Web Applications

Shahzad Ashraf*

College of Internet of Things Engineering, Hohai University Changzhou, China

***Corresponding author:** Shahzad Ashraf, College of Internet of Things Engineering, Hohai University Changzhou, China

Received: August 23, 2021 **Published:** August 30, 2021

Abstract

As the number of users interacting with dark websites grows, it opens the door for vulnerable and malevolent actors, making web traffic unsafe and risky. To prevent such vulnerabilities and maleficent activities on dark websites the proactive strategic measures have been taken into account and the relevant hidden causes are explored that helps to overcome the security risks during various web operations. In the first step, from the dark web corpus, the web addresses have been analyzed to check the status of whether these web addresses are available or not. To prevent the web addresses mining challenges a script was designed to mines irrelevant web address URL by visiting multiple search engines based on user input. In the 2nd step, another script was designed to check those domains having chances of becoming inactive because for security reasons such as onion sites. In 3rd step, various gape has been identified in dark web hosting using crawls that create the new links from configuration files. In the 4th step, using manual and automated testing the maleficent activities were identified in web traffic. Further proceeding to the 5th step, the web address lifespan was determined which quantifies the duration between the first and last occurrences of a web address. Finally, using Fisher's Exact Test (FET), two comparative scenarios have been developed by considering the similar attributes and the role of operating system interaction with surface and dark websites. In the first scenario for identifying the similar attributes of surface and dark websites, the role of maleficent and spammer has been investigated and found that overall, 86 and 800% of attributes of surface and dark websites are identical. Similarly, for 2nd scenario identifying how long the operating systems have interacted with surface and dark websites, it was found that windows, Linux, and android based operating systems have an incredible role and made the contents much pusillanimous which creates high chances of information leakage. In the end, up to 40 days of user interaction to surface and dark web has been analyzed and found various aggravated statistics regarding vulnerabilities involvement in network traffic such as maleficent, spammer and the information leakage. At the same time, the interaction period of operating systems with surface and dark websites such as windows, Linux, and Android is also statistically investigated. While gathering the aforementioned investigation it is observed that most of the websites use CMS, such as WordPress, Joomla, Drupal, and various forums, and are outdated with either no patching or having vulnerabilities. Since either, they hosted with old versions of the software or were not updated with the latest patches, most URLs in the dark web are vulnerable to attacks. After this study, clear and up-to-date statistics are unveiled regarding dark websites, and it is recommended that to get rid of vulnerabilities the obtained statistics can be considered before developing new applications

Keywords: Meticulous Testing; Vulnerabilities; Webhosting; Surface Web; Dark Web; Problematic Target; CMS; Script; FET

Introduction

The dark web is a section of the internet that can only be accessed using advanced routing mechanisms. The anonymity afforded to dark web users has been abused in order to engage in illegal online activity. Considering web security is a form of deafens nowadays and helps secure websites proactively for hosting in either surface web or the dark web. Securing a website is presently one of the most critical issues because of its significance in increased cyberattacks on the surface web. A crucial truth in web applications and their security is that a hosted web server and its related system cannot be entirely trustworthy, concluding that it cannot guarantee 100% safety [1]. All Web applications have their means, such as providing information and services. Web Applications interact with their backend known as (databases) several times per client request, and if the security of such websites and web applications is compromised, there could be outcomes in the form of information loss, financial loss, lawsuits, identity theft [2]. Cybersecurity must prioritize sustaining a productive computing environment and securing various transactions. Cybercrimes are on the rise across the world, and as a result, organizations, whether it is personal, a government which means it must be critical infrastructure. Not unexpectedly, the general state of web application security is highly conducive to cyberattacks [3]. Estimates indicate a

considerable number of online applications with security flaws and as a result, there have been several instances of successful security breaches and exploitations [4]. Organized crime thrives organically in this potential sector. Considering the millions worth of money made by such groups in the web's clandestine economy [5]. Security technology is insufficient to prevent web application flaws, and practitioners should focus on assessing and ensuring their success. This unindexed portion of WWW that intentionally hidden and inaccessible by standard browsers referred to as the dark web. Some Studies state that the surface web is only 4% of web content indexed by the publicly available search engines like Google, Bing. According to TOR metrics project, more than 200K registered. Onion-based addresses as of May 2020, and on average, daily 2 million users use TOR browser [6], to access the deep or dark web. The deep and dark web provides a venue for malicious actors to coordinate cyberattacks, illicit activities such as human trafficking and terrorist activities [7]. The main reason for using the dark web is its features such as encrypted protocols, anonymity, hidden in nature. While accessing the dark web, the dark web users encouraged neither the risk of getting caught by law enforcement nor being censored by a website [8]. The IP Address identifies a system as a unique identifier during Internet communication. It also aids in determining the geolocation of any device connected to the Internet. End-to- end device communication on the dark web, on the other hand, is encrypted by enabling anonymity of end devices, routers, and communication via the dark web [9]. The Law Enforcement Agencies (LEA) showing [10], an interest in the TOR-based network and its services mainly to understand the type of data hosted and their activities for any illegal activities. As the internet community grows, so do web dangers, nowadays majority of the illegal activities happen through the dark web, and it is tough to identify the criminals behind the activity. In this work, we carried out some vulnerability assessments on the dark web initially, and we mined numerous URLs from various sources such as search engines of the dark web. We gather information about the targeted host and use various methodologies. After that, we apply various vulnerability assessment methodologies, including manual testing of the web application and automated testing of targeted web applications and the result set presented in the result analysis. Dark web is one of the most challenging and untraceable mediums adopted by the cyber criminals, terrorists, and state- sponsored spies to fulfil their illicit motives. cyber-crimes happening inside the dark web are alike the real-world crimes. however, the sheer size, unpredictable ecosystem and anonymity provided by the dark web services are the essential confrontations to trace the criminals. The LEA required opportunities for tracing such criminals by using various methods [11]. By auditing and assessing the Dark Web, we can determine the availability of website availability and the information, which is sensitive, private, or potentially damaging information about an organization and related accounts, systems, and people. There are many monitoring methods, and we considered auditing and assessing applications, i.e., hosted websites on the dark web.

The main contribution of this study includes the following findings.

- Monitoring for breached usernames, passwords and other information.
- The Business resources and secrets which are breached and put up on sale.
- Monitoring the specific websites based on technical changes, transactions in their business, and relevant illicit activities.

Rest of the manuscript is arranged as: The literature review has been placed in "Related work section, and the proposed proactive methodology has been explained in "Proposed proactive strategy" section. The section "Dark web data selection strategy" highlights the current hurdles to the webhosting system. The overall access duration with surface and dark websites has been investigated in "Comparative scenarios" section. The results have been critically discussed in "Result and discussion" section. Finally, work has been concluded in "Conclusion" section.

Related Work

Due to the increasing number of web applications in both the surface web and the dark web, the corresponding numbers in sophisticated threats are also increasing. There are requirements to understand vulnerabilities or gap areas to check about creating new tools that are efficient and accessible becomes essential. The researcher in [12], describes a validation study in which participants answered quiz questions using the tool prototype, the sample data generated using the OWASP ZAP scanner tool, and a prototype implemented and used for validation purposes. They discussed the Web forensics and legal aspects researcher collected criminal files which have been investigated with official permits and crime models that will create the database have been determined. These crime models are conventional crimes committed through web activity or cybercrimes.

Another author [13], presented an insight into various aspects of the Dark Web, such as features, advantages, disadvantages, and browsers. Further, they discussed the different types of attacks, exploits, and malware with an overview of different types of criminal activities and incidents over the dark web. Many web applications in the dark web deal with a vast amount of secure and high transactions. As a result, security plays a significant role in web application development for the dark web too. The security of any web application focuses on the data the application handles, where the Audit and Assessment of web applications in the dark web may give some idea of understanding risks, and it may help investigators trace illegal activities. Further [14], discussed the suggestions provided in this article are in line with the majority of experts. In addition to the results, there are several typical IT issues in the network security of institutions. It is important to highlight the need of performing a risk analysis before exploiting

vulnerabilities. These are answers for the time being but will become weaknesses in the future, necessitating improved tactics. Defend against cyber-attacks. Another researcher [15], discussed the vulnerability assessment as it is useful since it gave information on the security of the websites that were chosen. Vulnerabilities were identified in all of the examined web servers. Some vulnerabilities were discovered across all web hosts, while others were exclusive to a single host. These revelations revealed that there are security concerns that need to be addressed across the board. On the same ground [16], discussed and suggested a unique approach for injecting realistic assaults into web applications automatically. This approach entails evaluating the web application and creating a list of probable flaws. After that, each vulnerability is injected, and numerous assaults are launched against it. Each attack's success is automatically analyzed and reported. One of shrewd approach by [17], looked at the issue of selecting appropriate SATs for web application vulnerability detection. They proposed a method for developing benchmarks for evaluating such SATs at various levels of criticality. In four situations of escalating criticality, they use SCM to automatically arrange the workload. To rank the tools in each situation, several measures are used. Saiba nazah [18], in presented a comprehensive examination of the visible section of the darknet's structure and content they were the first to methodically (recursively) investigate the visible darknet's network topology. The author [19], discussed the threat landscape is complex and ever-changing. To deal with the size of the pentest, autonomous solutions are required. Autonomous Security Analysis and Pentesting (ASAP) is an effort toautomate attack analysis, attack plan generation, and validation. Future Work: Using host logs to develop the AI model and attack plans for the visible darknet's network architecture. Similarly [20], developed MASSDEAL, a tool for the automated exploration of the Dark web that learns about new or previous unseen services and measures repeatedly across time where they collected data over more than 20 thousand dark web services sampled from September 2018 to January 2019. The performed an extensive analysis of service redundancy and measure the appearance of. onion mirrors as well as providing an estimation of the infrastructural redundancy behind those systems. Considering the same opinion, the [21], performed and analyzed the text content of 28,928 HTTP Tor hidden services hosting 21 million dark webpages and confirmed 901 phishing domains They conducted mainly an in-depth measurement study to demystify the prevalent phishing websites on the Dark Web to understand the dark web trends. This trend exacerbates the risk of phishing for their service users who remember only a partial TOR hidden service address. This study is about the auditing of websites on the dark web, in identifying vulnerabilities and gap areas, where they can support LEA for monitoring requirements to identify various activities of a website. We tried with lesser number of websites and achieved indented results for further to extend our research in building the classification framework for dark web sites.

Proposed Proactive Strategy

the proactive strategy is being conducted to analyze the impact of maleficent elements on websites hosted on the dark web. All such websites have been tested from different locations while keeping in mind that these websites were not in normal status and therefore, the alternate workstations were used in order to avoid any unusual situation as illustrated in Figure 1. During testing period, the multiple vulnerabilities were identified in various categories such as Adults, Drugs etc. Around 650 websites were tested from www web corpus and more than 60% of websites found to be vulnerable and unprotected from various attacks. During this operation, the different activities were performed in order to get the desired outcome which eventually turned the activities into a proactive strategy.

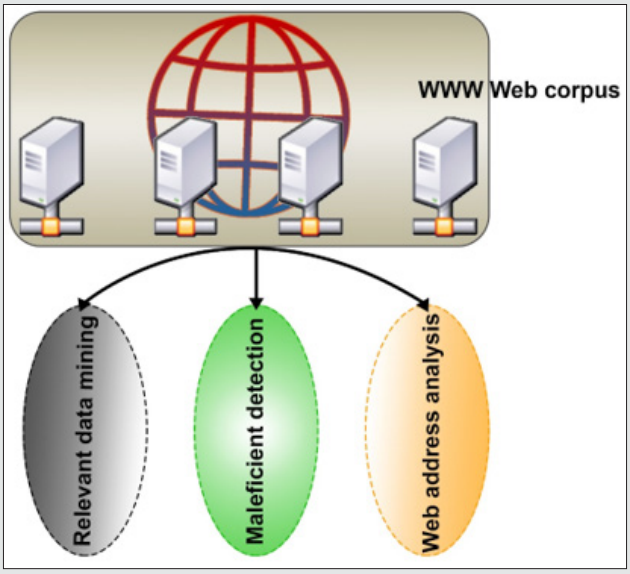

Figure 1: Proactive research methodology.

Relevant data mining

During the operation of dark web data mining, some indexing related uncouth situation was occurred because the addresses of the dark web do not appear in normal format. Further, web address belongs to dark web are exceptionally complicated and employs a more robust and modern encryption algorithm. It is much hard to recall the web address belongings to the dark websites due to URL length as 56 bytes long. These features make mining challenging; therefore, for a proactive strategy a script was designed that mines the URL by visiting multiple search engines based on user input and creating a unique result set. In addition, live activities were performed to catchup all those domains that having chances of becoming inactive because for security reasons, onion sites may become inaccessible after some time. Another script was designed to forecast the status of onion domain active or not, and also it reverts the status code (200,301,404,403 etc.), the title of the web page and saves results if the domain can redirect to some other domain [22]. Further, it is crucial identifying the gap for dark web hosting and every aspect is needed to investigate the areas which were ignored. Spiders/ crawls can use different techniques, such as brute force, to discover vital files or configuration files that have been missed or concealed. A SOCKS proxy is used to establish connections to the hidden services by the crawlers, which are written in Python. The crawler receives the first onion domains or seeds from the surface web's publicly available directory. A separate file is created for each seed that is scraped and the new links that are discovered. The new links were crawled again to find other new links. The scraping of new link is performed two more times until no new connections can be identified. The crawler did not scrape hidden services that required user authentication or were behind subscription pay-walls. Getting the user information such as email address, phone address, how generally the users act, details about the admin, all are required and therefore, information gathering also includes looking into exposed tokens, API endpoints, API entry points, and reading the parameters. The API is used to find login information in files; client-side validation is available, although it is preferable. Having as much knowledge about the target as possible makes work more accessible and manageable. Therefore, all potential hostnames connected to target and relevant open ports have been considered. The domain-level structure of the dark web has been examined, and all sub-domains of a certain domain are aggregated under it and indicated as a single individual node of a graph. The onion possessing two sub-domains en.ABC.onion and my.IMS.onion [23], each of these sub-domains and their internal web pages are considered as a single node of graph identifiable by respected domain name. As a result, each edge in the graph connecting nodes A and B symbolizes a hyperlink inside domain A's web page referring to a web page included in domain B.

Maleficent detection

The web maleficent detection is a complicated process of identifying vulnerabilities in web traffic; the loopholes are a significant cause of data breaches, hacking, and ransomware, among other things. The information gathered was utilized to start the maleficent detection of the web hosts Two techniques are used for this detection i.e., manual testing and automated testing. As a result of the manual testing being conducted by humans, it is essential that the testers think like a hacker. The tester examined each component of the target by hand and used a variety of methods based on his expertise of how to defend it. Automated testing makes use of scripts, tools, and software to replicate the same process by repeating defined tasks. It is handy when viewing source code since it detects weaknesses and unexpected vulnerabilities immediately. In automation testing, software such as ZAP, Burp Suite, and others are utilized [24].

Web address analysis

It has been determined that web addresses have a life expectancy, which is a novel classification. The concept of the invoked web address lifespan has been added, which quantifies the duration between the first and last occurrences of a web address in a data collection. It is related to the dynamics of content interest on the dark web. This notion is applicable to a variety of hosting considerations, as well as online cache activities. A simple parametric function closely linked to the probability density function well approximates the distribution of invoked lives. A unexpected finding was made using this model: the anticipated lifespan of a web address is asymptotically equal to the time frame of observation. It's also surprising to see a classic and well-behaved web family of statistical distributions at all [25]. This is particularly noteworthy since a substantial volume of web addresses in online traffic are nonces inside the scope of web data corpus. Furthermore, the structure inherent in web addresses was evaluated by comparing the use of path hierarchy vs query string on a range of dark sites. Surprisingly, static material is supplied via a path-depth structure, whereas query parameters include personalized content. Despite the fact that the two morphologies are functionally similar, there is a path-depth versus query-parameter dichotomy. Also, a web address does not have to represent the content of the resource if it is not used for search and resource discovery or is handled in another way. As a result of the widespread usage of query strings in many applications, the web address is no longer viewed as a simple node in a hierarchical file system [26].

Dark Web Data Selection Strategy

While exploring the dark web for data collection, it was much hard to find the appropriate data as most of the time accessibility issue hurdles reaching to specific hosted data. An obscure part of the Internet that can only be accessed with special software is known as the dark web Although there are several dark web technologies, they all have the feature of employing encryption [27], to provide anonymity.

Dark web alive time

When it comes to selling illegal items and services, most dark web sites, also known as dark markets, are similar in functionality

and structure to other well-known websites. They provide a wide range of illegal commodities and appear to cater to customers seeking specific content. As a result, one cannot be certain if the dark web will be accessible online or not because web addresses for such websites are not available throughout the session.

Maleficent detection is a time-consuming process that might take anything from many hours to several days to finish [28]. There is no guarantee that a website will be available during the maleficent assessment task. In the same way as ordinary websites, dark websites are linked to one other and to each other. When webpages did not have hyperlinks, users had to know the precise URL to find them. Thus, hyperlinks serve as the foundation for how users navigate this network, connect to domains, discover information, and interact with other users. Using social network analysis, these linkages may be examined, revealing the web's connections [29]. In the dark network, websites with more inbound and outbound hyperlinks may be regarded more popular and significant for the dissemination of information inside the dark network, Network analysis may assist in determining not just how information is transmitted and exchanged within network structures, but also the significance of certain websites to the network. A tiny dense cluster [30], of nodes, similar to other Internet topologies, may constitute the network's hub and direct the flow of information. Significant ramifications for how communities grow and operate might result from this, as could the tactics employed by law enforcement authorities to discover and remove unlawful users and material. Similarly, considering the web address delay response, the time it takes the web application server to complete one request is referred to as latency. Congestion has crept into the dark network [31], and the flow management system has failed to keep up with it. The issue of high latency is not the only one that has to be solved. Furthermore, the dark network is quite variable. Because queries are routed via several computers across the world, the dark network will never be as fast as the surface web. As a result, network latency will always be a problem. It took a long time to examine the endpoints and other features of websites since there were numerous instances of web address delay. An excessive amount of HTTP requests was made to the web-based application server because of this high delay rate. Further, checking some static web sites on dark web environment, Many CMS-based websites [32], are challenging to evaluate since the community is always working on security fixes and looking for new vulnerabilities. It has also been discovered that several hidden websites have not been updated.

Comparative Scenarios

In order to examine the roots of the dark web hosting script, the comparative scenarios are developed which enhanced the chances of getting accurate data and presages upcoming attacks.

(i). Similar attributes: The principles of running a web environment are the same on the surface and dark webs because Onion services are the part of the dark web, it does not expose the host's IP address but on the surface web, the IP address is accessible to everyone, therefore a misconfiguration can reveal the server's IP address [33]. When comparing the characteristics of the surface and dark webs, the dark web was found to be misconfigured. Exploiting a dark web site, as in the surface web, might disclose dark web users who visit the dark web site. As a result, identifying a surface web site relevant to a dark web site based on ownership and developer can increase the odds of understanding the user's activity. The Fisher's Exact Test (FET) [34], was used to assess the connections between surface and dark websites. The FET confirms the strong correlation between the web environment and maleficent. Unlike the dark web (1%) where this occurrence is rare, the surface web (12.2%) is more likely to experience the maleficent than the dark web (1.3%) shown in Table 1. It was discovered through a more detailed study that this relationship is only significant in paste locations. As a result of this, attackers on the dark web may be stealthier and try to avoid detection by not changing passwords on their accounts, indicating a certain degree of skill. The observed variations in the underground forums are insignificant.

Table 1: Comparative attributes of surface and dark websites.

Hosted sites	Maleficent (%)	Spammer (%)	Overall (%)	FET output
Surface	17	0.1	86	$p < 0.002$
Dark	2	3.8	800	
Hosted Forums				
Surface	4.8	2.1	77	$p < 0.091$
Dark	1.3	0.1	101	

(ii). Operating system and dark web pusillanimous contents:

The conflict between operating system and dark websites have been analysed and around 600 websites were test having malicious infectives. Further, the CMS [35], based applications such as WordPress, Joomla, Drupal, and others, found attacking via outdated plugins are also checked. [Table 2] depicts the distribution of web environment and operating system in each situation in which credentials were exposed. When credentials are collected during site operation, there is a strong link between the operating system and the dark web environment. This connection, however, is tenuous. Although the majority of the accesses come from windows, the study found that hackers are more likely to utilize android devices when utilizing credentials obtained via the surface web than the dark web (22 % vs. 2 %, p 0.001). As the users are likely utilizing their own mobile devices to access the accounts, this might be a sign of a low degree of sophistication. Linux, on the

other hand, is more likely to be utilized in the dark web (30% vs. 5%, p 0.001). According to the dark web's complexity, it is logical to infer that criminal who utilize Linux are more experienced. With regard to underground forums, there is no discernible difference. Sometimes using same web template might cause to vulnerabilities due to ignorance and insufficient knowledge about technologies and motivation about security. Exposing websites are not automatically updated and must be updated manually as popular CMS solutions frequently misconfigured and appealing target for hackers [36].

Table 2: Interaction of operating systems with dark websites.

Hosted sites	Windows (%)	Linux (%)	Android (%)	FET output
Surface	22	5	9.5	$p < 0.001$
Dark	2	30	8	
Hosted Forums				
Surface	0.1	8	0.1	$p < 0.034$
Dark	10	7.5	1.5	

Result And Discussion

The proposed proactive strategy unveiled very heuristic but interesting facts about web hosting contents. The proactive analysis time was set between July and August and near about 600 websites were tested on dark plate forum build on CMS based system and found that 95% websites developed by WordPress are massively maleficent and generating the vulnerabilities as depicted in Figure 2. Similarly, websites developed on Drupal has 66% ratio while Joomla, Wix, and Kentico shares 46%, 39% and 17% ratio respectively. These statistics vouched that how much CMS system is unsafe and risky!

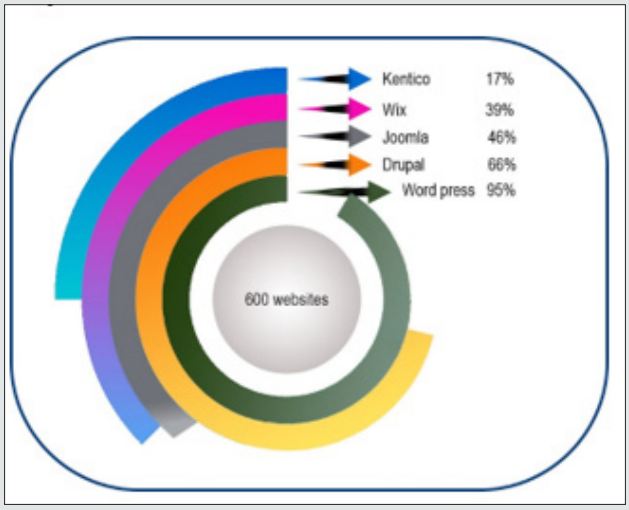

Figure 2: CMS based vulnerabilities analysis.

(i). Surface and dark web access duration: Furthermore, user behavior in terms of surface and dark web access duration has been identified, with activity lasting up to 40 days as illustrated in Figure 3. During first 20 days, users accessed the surface websites for up to 50 FET, with a total of 30% maleficent cases of the resource, while spammer problems and information leakage concerns remained at 12 and 21%, respectively. Users, on the other hand, have accessed dark websites, and access time reaching up to 72 %. Meanwhile, maleficent, spammer, and information leakage issues have reached new highs of 35 %, with spammer activity remaining low at 8%, but information leakage duration staying high. According to data collected over 40 days, surface and dark web accessibility remained almost the same, while overall network operation remained high risk. Maleficent, spammer, and information leakage activities for the surface web remained at 21, 29, and 16 %, respectively, during these days. Spammers have been observed to make extensive use of network resources, which could be as a result of users continuing to subscribe to websites and putting themselves at risk. Although the dark web's access time was almost the same as the surface web's, there was a slight decrease in the number of malicious and spamming activities, but the amount of information leakage was higher than the surface web's access time.

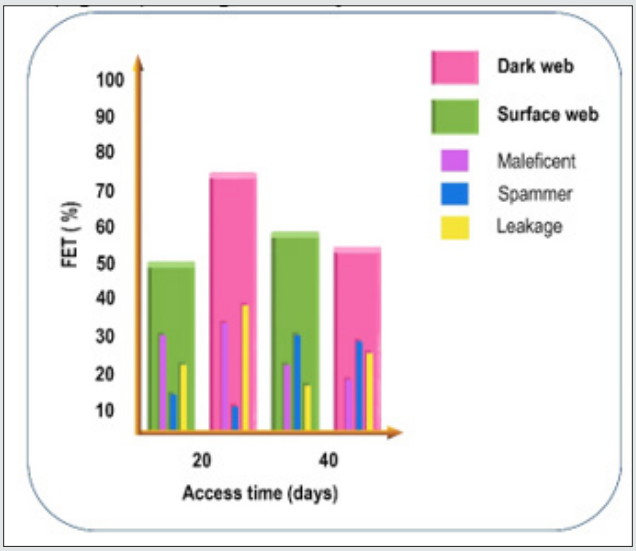

Figure 3: Surface and dark web accessibility.

(ii). Operating system interaction to surface and dark websites: The interaction of various operating systems, such as Windows, Linux, and Android, with surface and dark websites was also explored for entire 40 days and shown in Figure 4. The surface and dark web access durations were remained 80 and 58% respectively, during first 20 days. These websites were accessed using Windows, Linux, and Android operating systems, and unfortunately, the interaction between these operating systems was aggravated by 75, 39, and 72 % for surface websites, respectively. The interaction between Windows and Android was nearly identical, indicating that users of both operating systems have easy accessibility to surface websites. When users accessed the dark website on the same days, it showed that they interacted with it more on Windows than on other platforms such as Linux and Android. However, as Android users grow, their role can be seen during this activity. Similarly, for the next 40 days, a significant difference in accessibility between the surface and dark websites was observed, with 90 and 72 %, respectively. During these days, when accessing surface websites, the interaction with windows and Linux was nearly identical; however, while accessing dark websites, the windows and Linux interaction time was short, but they were competing with each other.

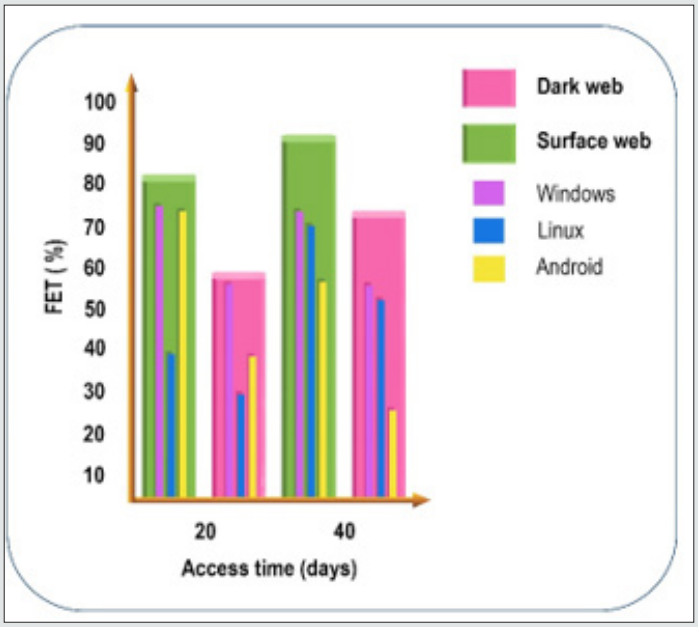

Figure 4: Operating system interaction with surface and dark web analysis.

Conclusion

In order to prevent the vulnerabilities and maleficent attacks while accessing the dark websites, a proactive mechanism has been proposed. This approach incorporates with users' behavior and by observing the surface and dark access time, the behavior of different unusual elements such as maleficent activities, the spammer role and the interaction of various operating system with dark and surface web has been studied. A dark web address corpus has been managed and the web addresses are analyzed to check the status about web URLs either available or not. Facing the web mining challenges, a script was designed to mines irrelevant web address URL by visiting multiple search engines based on user input. Similarly, another script was designed to check those domains having chances of becoming inactive because for security reasons such as onion sites. Further, various gape has been identified in dark web hosting using crawls that create the new links from configuration files. Afterward, using manual and automated testing the maleficent activities were identified in web traffic. Eventually, the web address lifespan was determined which quantifies the duration between the first and last occurrences of a web address. At the end, using Fisher's Exact Test (FET), two comparative scenarios have been developed by considering the similar attributes and the role of operating system interaction with surface and dark websites. In the first scenario for identifying the similar attributes of surface and dark websites, the role of maleficent and spammer has been investigated and found that overall, 86 and 800% of attributes of surface and dark websites are identical. Similarly, for 2nd scenario identifying how long the operating systems have interacted with surface and dark websites, it was found that windows, Linux, and android based operating systems have an incredible role and made the contents much pusillanimous which creates high chances of information leakage. In the end, up to 40 days of user interaction to surface and dark web has been analyzed and found various aggravated statistics regarding vulnerabilities involvement in network traffic such as maleficent, spammer and the information leakage. At the same time, the interaction period of operating systems with surface and dark websites such as windows, Linux, and Android is also statistically investigated. While gathering the aforementioned investigation it is observed that most of the websites use CMS, such as WordPress, Joomla, Drupal, and various forums, and are outdated with either no patching or having vulnerabilities. Since either, they hosted with old versions of the software or were not updated with the latest patches, most URLs in the dark web are vulnerable to attacks. After this study, clear and up-to-date statistics are unveiled regarding dark websites, and it is recommended that to get rid of vulnerabilities the obtained statistics can be considered before developing new applications.

References

1. W Park (2020) A Study on Analytical Visualization of Deep Web. 22nd International Conference on Advanced Communication Technology (ICACT) pp: 81-83.
2. S Ashraf, D Muhammad, Z Aslam (2020) Analyzing challenging aspects of IPv6 over IPv4. Jurnal Ilmiah Teknik Elektro Komputer dan Informatika 6(1): 54.
3. S. Ashraf (2020) Bodacious-Instance Coverage Mechanism for Wireless Sensor Network. Wireless Communications and Mobile Computing 2020: 1-11.
4. X Du, Q Le, M Scanlon (2020) Automated Artefact Relevancy Determination from Artefact Metadata and Associated Timeline Events. in 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security) pp. 1-8.
5. S Ashraf, S Saleem, A H Chohan, Z Aslam, A Raza (2020) Challenging strategic trends in green supply chain management. International Journal of Research in Engineering and Applied Sciences 5(2): 71-74.
6. S Saleem, S Ashraf, M K Basit (2020) CMBA - A Candid Multi-Purpose Biometric Approach. ICTACT J Image Video Process 11(1): 6.
7. S Ashraf, S Saleem, T Ahmed, Z Aslam, D Muhammad (2020) Conversion of adverse data corpus to shrewd output using sampling metrics. Vis Comput Ind Biomed Art 3(1): 19.
8. S Ashraf (2019) Culminate Coverage for Sensor Network through Bodacious-Instance Mechanism. i-manager's Journal on Wireless Communication 8(3): 9.
9. S Ashraf, T Ahmed, Z Aslam, D Muhammad, A Yahya, et al. (2020) Depuration based Efficient Coverage Mechanism for Wireless Sensor Network. J Electr Comput Eng Innov JECEI 8(2): 145-160.
10. Pratibha, A Gahalot, Uprant, S Dhiman, L Chouhan (2020) Crime Prediction and Analysis. in 2nd International Conference on Data, Engineering and Applications (IDEA) pp. 1-6.
11. S Ashraf, T Ahmed, A Raza, H Naeem (2020) Design of Shrewd Underwater Routing Synergy Using Porous Energy Shells. Smart Cities 3(1): 74-92.
12. S Ashraf, D Muhammad, M Shuaeeb, Z Aslam (2020) Development of Shrewd Cosmetology Model Through Fuzzy Logic. International Journal of Research in Engineering and Applied Sciences 5(3): 93-99.
13. S Ashraf, T Ahmed, S Saleem, Z Aslam (2020) Diverging Mysterious in Green Supply Chain Management. Orient J Comput Sci Technol. 13(1): 22-28.
14. A Shahzad, A Tauqeer (2020) Dual-nature biometric recognition epitome. Trends Comput Sci Inf Technol 5(1): 008-014.
15. S Ashraf, M Gao, Z Chen, S Kamran, Z Raza (2017) Efficient Node Monitoring Mechanism in WSN using Contikimac Protocol. Int J Adv Comput Sci Appl 8(11).
16. S Ashraf, S Saleem, S Afnan (2020) FTMCP: Fuzzy based Test Metrics for Cosmetology Paradigm. Adv Comput Intell Int J ACII 4(7): 1-13.
17. S Ashraf, D Muhammad, M A Khan, T Ahmed (2021) Fuzzy based efficient Cosmetology Paradigm. 8: 513-520.
18. S Nazah, S Huda, J Abawajy, M M Hassan (2020) Evolution of Dark Web Threat Analysis and Detection: A Systematic Approach. IEEE Access 8: 171796-171819.
19. S Ashraf, S Saleem, T Ahmed, Z Aslam, M Shuaeeb (2020) Iris and Foot based Sustainable Biometric Identification Approach. 2020 International Conference on Software, Telecommunications and Computer Networks (SoftCOM) pp: 1-6.
20. S Ashraf, T Ahmed (2020) Machine Learning Shrewd Approach for An Imbalanced Dataset Conversion Samples. J Eng Technol JET 11(1): Art no 1.

21. S Ashraf, Z Aslam, S Saleem, S Afnan, M Aamer (2020) Multi-biometric Sustainable Approach for Human Appellative. CRPASE Trans Electr Electron Comput Eng 6(3): 146-152.

22. S Ashraf, T Ahmed, S Saleem (2020) NRSM: node redeployment shrewd mechanism for wireless sensor network. Iran J Comput Sci.

23. S Ashraf, S Saleem, T Ahmed (2020) Sagacious Communication Link Selection Mechanism for Underwater Wireless Sensors Network. Int J Wirel Microw Technol 10(4): 22-33.

24. S Ashraf, T Ahmed (2020) Sagacious Intrusion Detection Strategy in Sensor Network. 2020 International Conference on UK-China Emerging Technologies (UCET) Glasgow United Kingdom pp: 1-4.

25. S Ashraf, Z A Arfeen, M A Khan, T Ahmed (2020) SLM-OJ: Surrogate Learning Mechanism during Outbreak Juncture. Int J Mod Trends Sci Technol 6(5): 162-167.

26. A Shahzad (2020) Towards Shrewd Object Visualization Mechanism. Trends Computer Sci Inf Technol pp: 097-102.

27. S Ashraf, M Gao, Z Chen, H Naeem, A Ahmad, et al. (2020) Underwater Pragmatic Routing Approach Through Packet Reverberation Mechanism. IEEE Access 8: 163091-163114.

28. S Ashraf, A Raza, Z Aslam, H Naeem, T Ahmed (2020) Underwater Resurrection Routing Synergy using Astucious Energy Pods. J Robot Control JRC 1(5): Art. no. 5.

29. S Ashraf (2020) Underwater Routing Protocols Analysis of Intrepid Link Selection Mechanism, Challenges and Strategies. Int J Sci Res Computer Sci Engr 8(2): 1-9.

30. S Ashraf (2020) Underwater routing protocols: Analysis of link selection challenges. AIMS Electron Electr Eng 4(3): 234-248.

31. S Ashraf, M Gao, Z Mingchen, T Ahmed, A Raza, et al. (2020) USPF: Underwater Shrewd Packet Flooding Mechanism through Surrogate Holding Time. Wirel Commun Mob Comput pp: 1-12.

32. A Latinne (2020) Characterizing and quantifying the wildlife trade network in Sulawesi, Indonesia. Glob Ecol Conserv 21: e00887.

33. Z A Arfeen (2021) A comprehensive review of modern trends in optimization techniques applied to hybrid microgrid systems. Concurrency and Computation: Practice and Experience 33(10): e6165.

34. M A Khan, F A Dharejo, F Deeba, S Ashraf, J Kim, et al. (2021) Toward developing tangling noise removal and blind inpainting mechanism based on total variation in image processing. Electron Lett 57(11): 436-438.

35. A Ahmad (2020) Towards an Improved Energy Efficient and End-to-End Secure Protocol for IoT Healthcare Applications. Security and Communication Networks 2020 pp: 1-10.

36. S. Ashraf (2021) A proactive role of IoT devices in building smart cities. Internet of Things and Cyber-Physical Systems 1: 8-13.

DOI: 10.32474/ARME.2021.03.000157