DWPF: A Dark Web Pharma Framework for a more Efficient Investigation of Dark Web COVID-19 Vaccine Products.

Dr. Francisca A. Opoku-Boateng, CBFI
Dakota State University, Madison-SD

Abstract **-** The ongoing pandemic has posed a significant impact on the general well-being of individuals, exposing them to unprecedented financial hardships and online information deception. Additionally, it has forced consumers, buyers, and suppliers to look in the direction of a darkened economic world – the Dark Web (DW) – a place driven by financial gains and where illegal goods and services are advertised and sold. The DW is significantly aiding criminals to exploit the pharma industry's intellectual property e.g., flooding of fake Covid-19 vaccines. As the DW gains an increase in recognition by normal web users, how to perform cybercrime investigations on Covid-19 products like vaccines have become a challenge for manufacturers, investigators, and law enforcement. This research employed the Peffers et. al. design science methodology and aimed to understand the DW impact on the Covid-19 vaccine pharma product and created a four steps Dark Web Pharma Framework (DWPF). The DWPF was built upon the known Justine Nordine open-source framework template. Results indicates the DW knowledge on DWPF, usability, adaptability, and efficiency of the DWPF.

Introduction

Globally, as the COVID-19 pandemic persists, the need for humans to be provided with essential services and various commodities has been restructured. Several criminals across a broad spectrum – from inexperienced to experienced criminals who frequent the dark web - are leveraging the ongoing pandemic on impacted global society in terrible ways. On the dark web, a wide range of illegal activities, products, and services are sold. When it comes to Covid-19 vaccines on the dark web, there is a general lack of literature in this area hence grey literature (industry reports and expert interviews and non-peer-reviewed) publications were considered for this research. WHO cautioned consumers of these fake COVID-19 vaccines on the dark web (Miao, 2021). Even though the vaccines were readily available, poorly designed vaccination programs lead to long delays of individuals getting vaccinated (Kaspersky Team, 2021) as such, consumers turning to darknets. Based on expert opinions, pharmaceutical companies like JnJ, Moderna, Sanofi have confirmed there is limited knowledge on how the dark web operates and how to navigate it as there is a limited methodology that can be utilized by investigators to explore and navigate the dark web securely (D.G, 2021; C.V, 2021; F.H, 2021; Bracci, Nadini, Aliapoulios, McCoy, et al., 2021a).

Covid-19 Vaccines Current Investigations

- U.S Immigration and Customs Enforcement initiated ***Operation Stolen Promise*** **(OSP)** ***2.0***
  - Partnerships - As of March 2020 (only mentions Pfizer)
  - Investigation - HSI focuses on developing actionable intelligence and investigative leads
  - Disruption
    - Utilize its authority to dismantle fraud schemes and
    - Take down illegal websites (***no mention of Dark Web***)
  - Educating the public on various frauds and red flags on fake pharmaceuticals

- The road to successfully battle the Dark Web marketplace by investigators and law enforcement has resulted in no yield and proven futile (Baravalle et al., 2016)
- Dark Web frameworks have been proposed by researchers to:
  - Systematize investigations or investigative work (Narayanan, et al. 2020)
  - Concentrate specifically on distinguishing between specific kinds of contents relating to properties of TOR relays (Dolliver et al., 2018; McCoy et al., 2008)
  - Automating Dark Web scraping and analysis (Hayes et al., 2018)

Research Question

How can an open-source intelligence framework be leveraged for investigating pharmaceutical COVID-19 vaccine products on the dark web?

Research Objective

Ultimately create a dark web pharma investigative framework (that leverages open-source intelligence) which can be used by investigators.

Methods

Designing Science Guidelines – Peffers, et Al. (2007)	
Guidelines	Research Applicability
Problem Identification & Motivation	• Recognition of problem statement and as such proposing DWPF.
Define Objectives	• Designed the DWPF to aid in investigating fake Covid-19 vaccine products on Dark Web.
Design & Develop	• The Artifact - DWPF (in a form of a methodology).
Demonstration	• In this stage, the efficacy of framework was demonstrated.
Evaluation	• Quantitative – Expert Interviews (Grounded Theory Approach).
Communication	• Research outcome, its relevance to be published & presented.

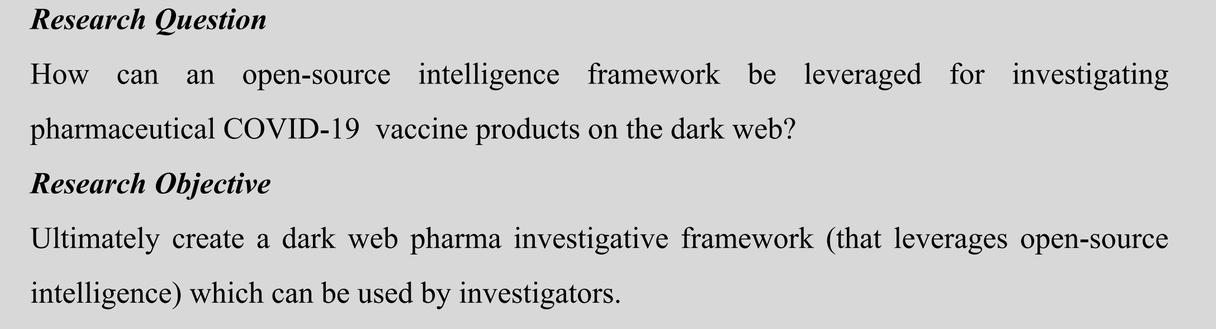

Figure 1: JSON Schema for DWPF

Results

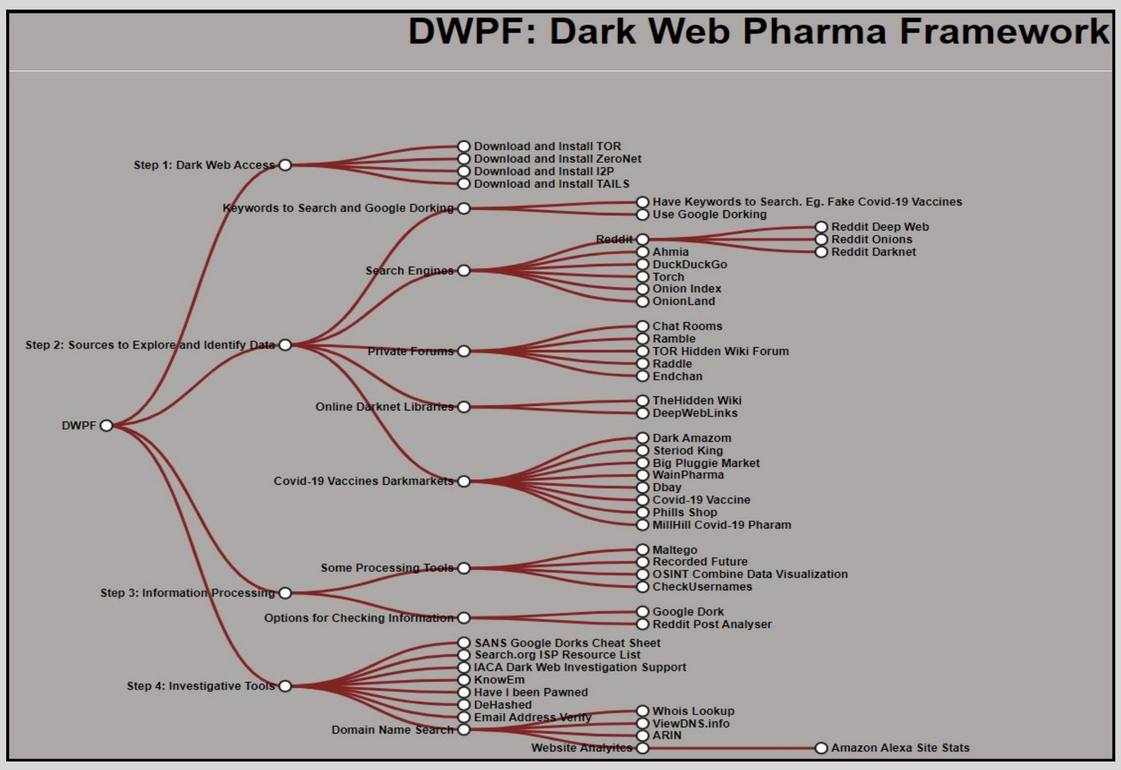

Figure 2: Fully Branched out DWPF

Discussion

- ***Theoretical Sampling*** **-** Small number of experts were recruited and interviewed. Data was collected, and initial analysis began after the data was transcribed.
- ***Open Coding*** **-** Transcribed data was broken down into excerpts. The excerpts were grouped into codes. The codes complemented each other.
- ***Axial Coding*** **-** Codes were grouped into the themes like usability, efficiency, and adaptability, and we tried to find the connection between the feedback information provided by experts to complete the final evaluation of the DWPF.

Dark Web Knowledge

DWPF 100% exposed experts to a handful of new dark websites they were not previously familiar with.

- ***P1 & P3*** " Tool is a very useful tool broken out step by step, re-confirmed the knowledge previously had prior to utilizing DWPF".

Usability

80% finds tool to be user-friendly and beneficial to their way of investigations.

- ***P1*** **"**the DWPF lets me find and explore different kinds of dark web resources all in one place. In one word, it is resourceful**"**
- ***P6*** **"**There aren't enough OSINT tools that enable COVID-19 pharmacovigilance. DWPF has summarized most of the tools needed for investigations in a simple to understand interface investigators can always use as a guide**."**

Efficiency

- ***P2*** **"**It is efficient because it cuts down time needed to search for all these resources by at least 85%**."**
- ***P4 & P7*** **"**Tools are listed and categorized well. Provides clear steps**"**

Adaptability

- 100% adaptable and must allow user to add on to resources.

Conclusion

The online market for covid-19 products like vaccines is rapidly evolving and due to the complete anonymity and security afforded by software such as TOR people feel more comfortable doing things that they would not dare do otherwise on the dark web. The objective of the research was achieved, as a Dark Web Pharma Framework (DWPF) investigative tool was designed leveraging several open-source intelligence resources and tools.

Contribution, Limitation and Future Work

DWPF offers a roadmap in the form of a decision tree-like display for investigators. Findings associates with work will serve as a source of reference. The applicability of DWPF to other products was a limitation but will be faceted into future works.

Acknowledgement

I will like sincerely thank my dissertation committee chair Dr. Cody Welu; and members, Dr. Kyle Cronin, Dr. David Bishop, and Cynthia Hetherington, HG.

References:

- Dolliver, D. S., Ericson, S. P., & Love, K. L. (2018). A Geographic Analysis of Drug Trafficking Patterns on the TOR Network. Geographical Review, 108(1), 45–68. https://doi.org/10.1111/gere.12241
- Hetherington Group. (2018, January 17). Matthew Golabek. *Hetherington Group*. https://www.hetheringtongroup.com/about/matthew-golabek/
- Kaspersky Team. (2021). *Coronavirus vaccines selling on darknet black markets*. https://usa.kaspersky.com/blog/coronavirus-vaccines-darknet/24286
- Baravalle, A., Lopez, M. S., & Lee, S. W. (2016). Mining the Dark Web: Drugs and Fake Ids. https://doi.org/10.1109/ICDMW.2016.0056