Dark Web InfoSec

Individual Research and Analysis

Naga Kartheek Peddisetty

MPS Data Science, University at Buffalo

2nd Semester

CDA 551LEC S4S: Cybersecurity, Privacy & Ethic

Dr. Arman Falahati

February 19th, 2024

Introduction:

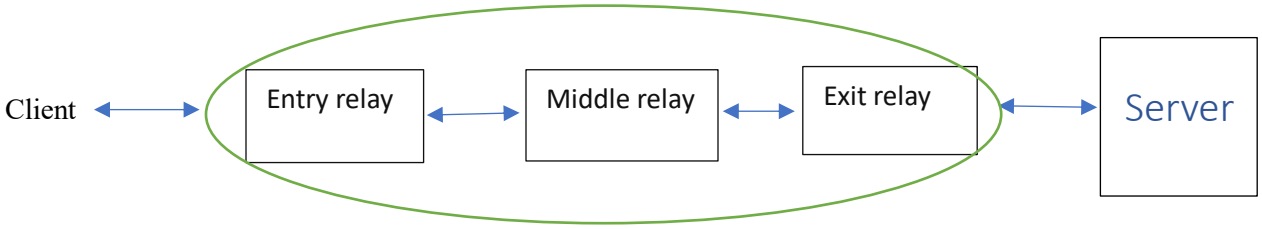
The Dark Web refers to encrypted online content and websites accessible only through anonymizing tools like Tor, which uses onion routing to obscure users' IP addresses. The Dark Web facilitates both legitimate aims like privacy and free speech as well as illicit activities like drug and weapons trafficking, child pornography, hacking, and more (Sugiu, 2017; Kristin, 2017; Nazah, 2020). However, investigating the Dark Web poses challenges due to anonymity protections.

Recent research has focused on analyzing Dark Web data to understand its scope, including through web crawling and domain classification (Faizan, 2019). Other work has examined the layers of the Deep and Dark Webs and reviewed literature on emerging crime threats enabled by the Dark Web anonymity. Criminals, terrorists, and state actors exploit the Dark Web for communication, coordination, and transactions often involving cryptocurrency. However, the extent of illicit activities is unclear (Kristin, 2017).

Methods to potentially deanonymize Dark Web sites and users are being developed but face hurdles. Recommendations include further analyzing crypto markets and forums, using anonymity services to aid investigations, and ensuring digital forensic techniques follow proper legal procedures (Nazah, 2020). Overall, more research is needed to identify effective and lawful techniques for combating Dark Web crimes while preserving legitimacy uses.

TOR (The Onion Router) Network:

The US Navy created the TOR network to safeguard internet communications. Subsequently, TOR was made available as open-source software, and it is currently run by the nonprofit organization The Tor Project, Inc. The TOR network is made up of routing software used to access the network, and a global network of volunteer computers that relay traffic. TOR bounces user connections through multiple relay nodes before reaching the destination, hiding the real IP address. This allows for anonymous surface web browsing, access to TOR hidden services, circumvention of censorship, and blocked content access. However, TOR has also enabled criminal activities due to the high level of anonymity. TOR exemplifies the dual-use challenge of privacy software being used for both legitimate and malicious purposes (Dr. Varin Khera).



Client: Software that encrypts user traffic and routes it through relays to conceal identity and location.

Entry relay: The first node that receives encrypted user traffic when connecting to Tor.

Middle relay: Intermediate nodes that further encrypt and forward user traffic through the Tor circuit.

Exit relay: The final node that forwards decrypted traffic to its internet destination.

Destination server: The ultimate internet destination that receives the traffic, seeing it as originating from the exit relay.

I2P (Invisible Internet Project):

I2P differs significantly from Tor in its design and implementation. Tor uses fixed size cells to transmit encrypted data, aiming to conceal hints about the content. I2P was inspired by onion routing but uses garlic routing - bundling onion cells of varying sizes with padding and delaying instructions into "garlic cloves". The variable size adds randomness against traffic analysis. Rather than circuits, I2P is message-based, with end-to-end encryption between users preventing attacks. Nodes repackage received cells into new cloves to forward. This makes I2P more resistant to timing and fingerprinting attacks versus Tor's circuit model. But both share building blocks of onion encrypted cells. The core difference is I2P's garlic routing and messaging focus rather than Tor's circuits (Bassam Zantout, 2011).

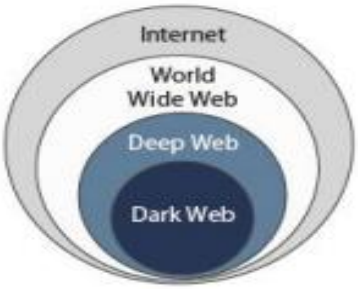
Layers of the Internet:

As we know, the web is one part of the Internet. The web is divided into three parts: the Surface Web, Deep Web, and the Dark Web. Search engines index the surface web, but not the deep web. The Dark Web is purposefully hidden, and it requires special software to access. The number of global Internet users exceeds 3 billion, but data on how many access the Deep and Dark Webs is unclear. The different layers of the web remain poorly understood (Kristin, 2017).

Surface web: The Surface Web is growing, with over 1 billion websites as of 2017. The magnitude of the overall web is difficult to estimate and constantly changing.

Deep web: The Deep Web's information is not indexed; thus, search engines cannot access it, making its extent impossible for estimation. However, it is believed to be thousands of times larger than the Surface Web and is rapidly increasing.

Dark web: The Dark Web within the Deep Web is expanding with new tools, but its scope remains uncertain. While offering anonymity, the Dark Web is used for both legal and illegal activities.



Layers of the Internet (Source: Dark Web, Kristin, 2017)

Criminal activity threats in the Dark Web:

1. **Human trafficking and sex trafficking:** Human and sex trafficking is rising due to online forums and the Deep Web's anonymity. Trafficking networks use the hidden nature to escape detection and recruit victims into forced labor, domestic employment, sex work, and more. In 2016, over 40 million people were victims of modern slavery, mostly women and girls trafficked into the commercial sex industry. Calls to human trafficking hotlines and trafficking convictions have risen, but many cases remain undetected due to the hidden nature of online networks (Nazah, 2020).

2. **Drug transactions:** The dark web acts as a hidden marketplace for drug trafficking, outside the reach of police. Sellers can sell narcotics anonymously, while purchasers can get illicit substances using bitcoin payments and hidden IP addresses. Despite law enforcement disruptions, new cryptocurrency markets emerge, selling everything from marijuana to heroin and cocaine. The dark web allows the drug trade to thrive across borders by connecting anonymous buyers and suppliers via encrypted networks hidden from the public internet. Despite being monitored, this digital black market is always creating new ways to satisfy harmful addictions and greed that are not limited by the law (Nazah, 2020).

3. **Child abuse:** The dark web hides the crimes of child exploitation. Hidden services appeal to criminals who share unlawful photographs outside the law. Despite efforts to disrupt networks such as freedom Hosting, new sites pop up advertising access to child pornography. Anonymity allows predators to operate freely, abusing the defenseless and feeding on demand. It is difficult to monitor these secret networks because criminals use encryption and bitcoin payments to avoid detection. While the dark web facilitates the worst crimes, it also requires law enforcement to develop new tools and collaborate globally to protect children from abuse and bring offenders to prison. This horrible trade continues to operate in the shadows, but determined defenders are fighting to bring it to light and put an end to it (Nazah, 2020).

4. **Terrorism:** The dark web provides a hidden environment for terrorist organizations to operate. Extremist groups such as ISIS use media to recruit and influence members beyond the government' control. Encrypted apps and Bitcoin donations allow for attack preparation, communication, and finance. Despite anti-terrorism efforts, new threats emerge in the digital underworld. Anonymity permits dangerous ideas to propagate and violence to be carried out undetected. This digital safety encourages radicals' darkest desires while also putting countries' resilience and free speech rules to the test. The dark web reflects both the light and dark aspects of human nature, making it beneficial and dangerous (Nazah, 2020).

5. **Markets for Cyber crime tools and stolen data:** The dark web enables hidden markets for cyber criminals to exchange hacking tools, stolen data, and other illegal products. Despite law enforcement disruption, new anonymous marketplaces continue to appear, using encryption and bitcoin to escape authorities. On the dark web, there are cat and mouse games as policing adapts to criminality made accessible by technology and anonymity (Nazah, 2020).

6. **Dark Net currency exchange using Bitcoin:** Bitcoin allows anonymous transactions on the dark web, free of official observation. Cryptocurrency empowers these secret markets that trade unlawful goods and services. Law enforcement investigates money laundering strategies to dismantle criminal organizations. However, the inherent privacy features of bitcoin, as well as the encryption of the dark web, make it difficult to track and enforce these operations. For the time

being, the dark web continues to exist by exploiting digital money and anonymizing tools to support undercover illegal activity (Nazah, 2020).

Summary:

The Dark Web refers to encrypted online information and websites that can only be accessed through tools such as Tor and I2P, which conceal users' IP addresses. It promotes both legitimate goals such as privacy and illegal actions such as drug trafficking, child pornography, and hacking. Investigating the Dark Web is difficult because of anonymity safeguards.

The TOR network uses onion routing to hide users' identities and locations. TOR allows for anonymous surface web browsing, censorship circumvention, and restricted content access. However, great anonymity has permitted illegal activity. I2P employs garlic routing and end-to-end encryption between users, making it more resistant to attacks than TOR's approach. However, both share the building blocks of onion encrypted cells.

Search engines index the Surface Web, but not the Deep Web, while the Dark Web is purposefully hidden and requires special software to access. The scope of the Deep and Dark Webs remains uncertain. And the Dark Web enables threats like human trafficking, drug transactions, child exploitation, terrorism, cybercrime markets, and anonymous cryptocurrency transactions etc.

Conclusion:

In conclusion, the Dark Web facilitates both legitimate goals and criminal threats by offering anonymous online communications. Methods for investigating Dark Web offenses while maintaining anonymity require balancing security and rights. More research and international cooperation is required to establish legal strategies for combating unlawful Dark Web operations such as trafficking and exploitation while maintaining free speech and privacy. Continuous monitoring and new techniques are essential to expose hazardous aspects of the Dark Web without compromising civil liberties.

References

Bassam Zantout, Ramzi A. Haraty (2011). I2P Data Communication System.

http://csm.beirut.lau.edu.lb/~rharaty/pdf/IC15.pdf

Dr. Varin Khera, Dark web & Internet Anonymity: Exploring the Hidden Internet.

https://cyberprotection-magazine.com/darkweb-internet-anonymity-exploring-the-hidden-internet

Kristin Finklea (2017). Dark Web.

https://a51.nl/sites/default/files/pdf/R44101%20(1).pdf

Mohd Faizan, Raees Ahmad Khan (2019). Exploring and Analyzing the Dark Web.

https://firstmonday.org/ojs/index.php/fm/article/view/9473/7794

SAIBA NAZAH, SHAMSUL HUDA, JEMAL ABAWAJY, MOHAMMAD MEHEDI HASSAN (2020). Evolution of Dark Web Threat Analysis and Detection: A Systematic Approach.

https://ieeexplore.ieee.org/abstract/document/9197590

Sugiu Takaaki, Inomata Atsuo (2017). Dark Web Content Analysis and Visualization.

https://dl.acm.org/doi/abs/10.1145/3309182.3309189?casa_token=e7nuJvEopT0AAAAA:_4voSaJs83_LII2rRoTA4zqwubtzMh_tyJi8t_5qqVSD9MgxigPcRYZOQxcYfmxug7GjDPwZXQw