

UNPROTECTED DATA: REVIEW OF INTERNET ENABLED PSYCHOLOGICAL AND INFORMATION WARFARE

Francisco GARCIA MARTINEZ

Illinois Institute of Technology, School of Applied Technology, Chicago, Illinois, USA
fgarciamartinez@hawk.iit.edu

Maurice DAWSON

Illinois Institute of Technology, School of Applied Technology, Chicago, Illinois, USA
mdawson2@iit.edu

ABSTRACT

Since the last elections in the United States, France, and other nations, fake news has become a tool to manipulate voters. This creation of fake news creates a problem that ripples through an entire society creating division. However, the media has not scrutinized enough on data misuse. Daily it appears that there are breaches causing millions of users to have their personal information taken, exposed, and sold on the Dark Web in exchange of encrypted currencies. Recently, news has surfaced of major social media sites allowing emails to be read without user consent. These issues bring upon concern for the misuse of data and more importantly, how can this be used for information warfare and the exploitation of targeted groups through the use of the Internet. It is essential that organizations continuously review current data policies to ensure that they do not become victims of information warfare.

KEYWORDS: data misuse, information warfare, Internet security, intelligence

1. Information Warfare

In the battlefield, there is a type of warfare known as psychological operations. This aspect of warfare is used to create a favorable image, gaining adherents, and undermining opponents had already become a significant weapon of 20th-century warfare. However, “*they are neither a substitute for power nor a panacea*” (Headquarters Department of the Army, 1979, pp. 1-5) but employed correctly they can be instrumental, making the difference between success or failure in military operations. And not exclusively military operations, but also in numerous other fields, such as technology or marketing.

Information warfare is, in general terms, a way of protecting one’s information infrastructure while attacking someone else’s by using computers. In the past century, it was commonly considered how future wars would take place and, more importantly, the mean by they would be won (Aldrich, 1996). Consequently, information warfare has become a significant issue in recent decades for both governments and private companies, who have often joined forces to strengthen their economies over their adversaries. For instance, in the United States, government agencies such as the Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI) or National Security

Agency (NSA) have cooperated with private organizations to create infrastructure protection programs (Elbirt, 2003). The term, whose first recorded use was by Thomas P. Rona of the Boeing Corporation in 1976, is of such a great importance that A. J. Elbirt (2003, p. 1) remarks in his paper that “*the International Trade Commission estimated the loss in the United States due to economic espionage at \$23.8 billion in 1987 and \$40 billion in 1989*”. Besides, a study conducted by the University of Illinois in 1988 concluded that 48 % of the companies surveyed admitted to being industrial espionage victims (Schawartau, 1997).

Typical information warfare attacks are a Denial of Service attack (DoS attack), phishing, social engineering, or deletion, manipulation or modification of data. All with the common goal of gaining a favorable position over their opponents by disrupting their services or stealing classified data. As a consequence, threatened by this information warfare attacks, the United States created in 1998 the National Infrastructure Protection Centre (NIPC). Typically, an attacker performs three steps when conducting an attack: information gathering, attack planning, and attack execution (Elbirt, 2003).

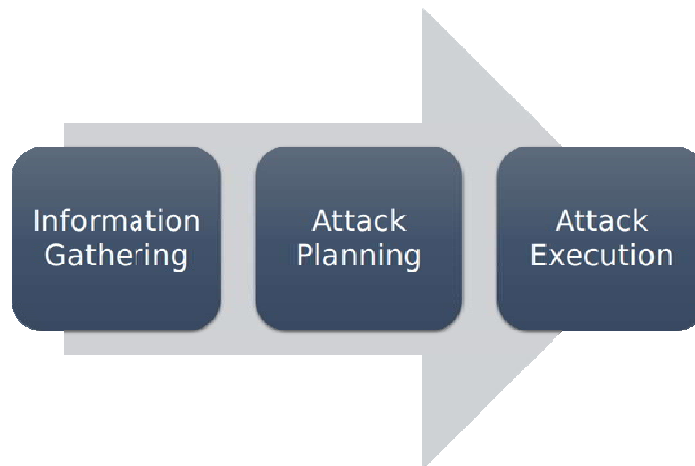


Figure no. 1: *Information Warfare Process*

The primary purpose is to retrieve as much information as possible from the adversary while protecting one's information infrastructure, thus ensuring confidentiality, integrity, and availability. From the economic point of view, there are three levels of impact in information warfare, being these personal, corporate, and global levels. The personal level affects a single individual or group of individuals electronic privacy. Attacks directed to the personal level include, but are not limited to, harassment, extortion, personal data theft or blackmailing. These kinds of attacks often consist of an individual's information gathering to, later on, perform a specific targeted campaign of blackmail or ransomware (O'Gorman & McDonald,

2012). Some other personal level attacks focus on unauthorizedly altering someone's private information. Though this misinformation could be easily removed or corrected, due to the extremely fast spreading of data across the network. Once an individual's privacy has been invaded, and the malicious activity has been done, the resulting damage is often irreparable.

When the conducted information warfare attacks are elevated to companies or organizations, they are often referred to as industrial espionage or the corporate level. The usual corporate level attacks involve competitor information theft, the release of their proprietary information, or disrupting an adversary's activity. Additionally, there have also been cases of

governments making use of Information Warfare tactics to provide information to a private organization within the country from a competitor of a foreign country. Elbirt gives an example of this kind of activity in his paper: *"Hitachi paid IBM a reported \$300 million in a settlement agreement after being caught spying on a new generation of IBM computer equipment and that French intelligence was proven to have spied on Boeing to help Airbus"* (Elbirt, 2003, p. 5).

Economic espionage, or global level attacks, refer to the government's use of Information Warfare techniques to combat other countries or their allies in the desire of improving their economy or obtaining a better combative position. Nonetheless, these attacks are not limited to government activities, but they also include terrorist groups, such as Anonymous, Al-Qa'ida, or the famous Chinese cyber espionage group, Axiom. However, they require a large number of people involved and a significant monetary investment. A key aspect of being successful at the global level relies on being capable of organizing this vast number of people while maintaining a high level of privacy.

Concerning data collection, databases can represent a great source of useful data within the information warfare. Numerous access control countermeasures have been developed and are implemented, preventing unauthorized users from accessing and retrieving confidential information. Nevertheless, those techniques do not address the inference control problem, where a user could perform legitimate general queries to the database as a whole while restricting him from extracting individual's private information (Elmasri, 2008). Clifton and Marks (1996) introduce some possible solutions in their paper. To ensure that a company cannot infer private data from public data to, later, use it to gain a better position than its competitors in the information warfare.

2. All Source Intelligence

Analyzing data could provide valuable information regarding an organization's or individual's activity with the use of Open Source Intelligence (OSINT) tools. OSINT data is unclassified information or data that is publicly available. OSINT is not to be a substitute for other sources of intelligence but rather complement existing methods to collect information such as Geospatial Intelligence (GEOINT), Signal Intelligence (SIGINT), Human Intelligence (HUMINT), and Measurement Intelligence (MASINT). This data collection method relies on information that is found publicly without the need to request access to it, and it can be used to generate reports (Stalder & Hirsh, 2002). Having access to this data allows an attacker to develop an intelligence analysis on the target. This analysis can be a culmination of information about the target's movements, online behaviors, technical data, and more. With the Internet, several applications such as Maltego can make the profession of an OSINT analyst done with ease. This means they can create transforms, perform sentiment analysis of words, and review other public databases with ease.

3. Misuse of Data

The widespread use of newer technologies and their correspondent tools and apps leads to infinite quantities of data released to the Internet. However, the most critical finding in the last recent years is that all this data has a value. All this information which was practically discarded was a source of intelligence that traditionally took a significant work effort to collect. Hence, enterprises have increased their investments in software, hardware, staff, education, and other associated items that constitute the digital world, by 50 %, to \$4 trillion (Gantz & Reinsel, 2011). Grantz and Reinsel state in their paper that *"the amount of information individuals create themselves – writing*

documents, taking pictures, downloading music, etc. – is far less than the amount of information being created about them in the digital universe” (Gantz & Reinsel, 2011, p. 1). Therefore, we cannot imagine how significant this amount of data is, and even less wonder how to handle it. That is why companies are putting all their efforts to be able to generate value by extracting just the right information, or even by misusing the data for different purposes for what it was collected. Being capable of doing so would enormously help to position themselves in the “pole position” of the information warfare.

It cannot be denied that the new features included in popular apps usually make someone’s life easier. However, the actual goal of the company for developing that new functionality remains unthinkable and unknown to the end user. These goals can range from the selling of data to third parties or collecting data to sell other products to the end user (Ahmed, 2004). It was probably not to make everyone’s lives more comfortable but to know more about them; to gather more useful information about the people which can later be transformed into personal-oriented marketing strategies and, eventually, more revenues to the corporation. What enterprises usually achieve with these techniques is to get more private information about their users’ data, or metadata, which, as a result, is growing extremely faster than the actual data itself. In recent years several patents can be found that deal with mobile data collection to (Sinisi, 2007). Facebook’s new “face recognition” or “tag suggestion” feature is an excellent example of this. This functionality identifies a user’s face in a picture and notifies him of the uploaded photo. Thus, the user can decide whether to be tagged in the photo or, even more, report someone who has

uploaded a picture of him without consent. Although several privacy experts claim that it is an excellent advance in protecting someone’s privacy preventing fraud and identity theft, what Facebook does is maintaining what it is called a “template” (Fussell, 2018). This template is a string of numbers that is unique for each user, which could be considered similar to a fingerprint. As a consequence, Facebook becomes the owner of extremely protected biometric data of its customers, that could later be tasked for malicious purposes.

According to John T. Soma et al. personally identifiable information (PII) *“is now a commodity that companies trade and sell”* (Soma, Couson & Cadkin, 2009, p. 1). Furthermore, it is equaling or even surpassing the value of traditional financial assets in large corporations. Nevertheless, the question is: are companies benefitting from the use and trade of PII without protecting the privacy interests of those PII owners? This entails consequences for commercial and technological sectors.

In the marketing industry, the benefits of using PII are double (Soma, Couson & Cadkin, 2009). Imagine that an online store sells alcohol to its consumers. Collecting data such as gender or nationality may not make any difference, but, if it also collected age values, it could significantly narrow its target to old enough consumers. Thus, the store would not only increase its revenues by approaching more likely possible buyers but also reduce costs by discarding underage consumers. Moreover, consumers can also benefit from companies keeping their PII, tailoring them future activity.

Cloud computing is becoming an excellent solution for many small and medium companies since it represents a great way of saving money by sharing resources with other organizations and

avoid buying and maintaining their servers. However, regarding security, cloud providers may have to face different risks and challenges to the ones in conventional IT environments. From the end user's point of view, they are still reticent to cloud computing technologies, concerned about their data privacy and security issues — even more after knowing about the most significant cloud computing providers security breaches. Google Gmail was exposed to a severe vulnerability up to 4 hours in its VMware virtualization for Mac version in 2009, where attackers could take advantage of this vulnerability to execute malicious code on the host (Chen & Zhao, 2012). Microsoft Azure also suffered a severe outage accident on its cloud services for 22 hours earlier this year.

Concerning the health sector, due to the augment of health information available in the Internet, patients tend to look for their symptoms online, sharing especially private data to everyone, without considering its associated security risks. Researchers comment that *“Both specialists and patients can benefit from linking family health profiles so that all relevant information is available for reference when the need arises”* (Gajanayake, Iannella & Sahama, 2011, p. 31) obviously, developing a safe and private environment. The access of illegitimate persons to one's health information can have critical consequences when later being disclosed or misused since it contains sensitive data tremendously useful for ransom ware or social engineering attacks. Thus, they propose an information accountability mechanism as the solution to information misuse in the health field. Moreover, they claim that with their approach *“when inappropriate misuse is detected, the agent defines methods of holding the users accountable for misuse”* (Gajanayake, Iannella & Sahama, 2011, p. 37).

4. PII Exploits

Krishnamurthy and Wills define personally Identifiable Information (PII) as *“information which can be used to distinguish or trace an individual's identity either alone or when combined with other public information that is linkable to a specific individual”* (Krishnamurthy & Willis, 2009, p. 7). The term encompasses any information that can uniquely identify an individual, such as name, birthday, address, phone number, social security number, fingerprints, or a face photo.

Social networking sites are web-based services that allow their members to build a public or semi-public profile and connect with other strangers based on shared interests, hobbies, or political thoughts (Boyd & Ellison, 2007). We could say that social media is an expansion of traditional media, offering individuals highly capable and nearly unlimited ways of communicating and networking with others. There are many different kinds of social media business models, varying from sharing live-photos of places you are currently visiting activities focused on growing your professional network and seek jobs. Nevertheless, just like everything in this world, social networking sites also have their drawbacks. Users do not often realize the massive amounts of personal data that they are sharing with their network and thus, how they are being exposed to exploits of these data.

All social networks offer a wide range of possibilities concerning the privacy settings of their members. If an individual leaves these settings public by default, this can constitute a breach of privacy. Consequently, a malicious user can perform a reconnaissance attack and gather as much possible information to conduct a successful social engineering attack later.

However, having a public profile is not the only vulnerability to private information on a social networking site. In their paper, P. Gundecha et al. discuss how a social media user can become way more exposed to exploits of his data by merely adding a vulnerable friend. They define a vulnerable friend *“from an individual user’s perspective is dependent on whether or not the user’s friends’ privacy settings protect the friend and the individual’s network of friends (which includes the user)”* (Gundecha, Barbier & Liu, 2011, p. 511). Hence, a single user’s privacy settings can compromise its entire network.

Frequently, social media websites partner with third-party servers to provide content and advertisements to their users. Although these websites claim in their privacy policies that they share cookies to third parties to offer a better user experience to their members, these cookies do not exclusively consist of Internet Protocol (IP) addresses (Symantec Corporation, n.d.). What is more, some third-party servers are in fact trackers or aggregators, that follow the user habits before, while and after the user’s interaction with the social media application (Krishnamurthy & Willis, 2009). Krishnamurthy and Willis define this action of combining this PII with other information and sharing it to external websites as “leakage”. In their paper, they present a study demonstrating how Online Social Networks (OSN) often provide information linked to a particular person to third parties via a combination of HTTP headers and cookies.

Most of the times, when a person publishes a document or picture on the Internet, he is not aware of the PII or other identifiers attached to it, even less how to remove them. There are countless situations in which personal information is retrieved from documents with inappropriate security. Therefore, this private data can further be used to commit malicious

activities. An example of information leak caused by inadequate attempts to secure protected information took place in 2000 when a secret CIA document about a coup in Iran was published in The New York Times website (Aura, Kuhn & Roe, 2006). The company unsuccessfully tried to erase the names of the persons involved by just painting white squares over their names. As a consequence, the names were still in the publication’s metadata and could easily be retrieved.

5. Where Stolen Data Can Be Found: Dark and Deep Web

The types of data captured through poor security practices and improper coding techniques provide not only side channels into the organizations but a plethora of details. For example, a photo provides lots of metadata that can give insight into camera type, specific detailed information of photo taken, latitude, and longitude coordinates. These items can be used to create an intelligence analysis of a target with the number of connected devices and those on the Web with a lack of security protections. However, the key is where these stolen data and information end up do.

The definition of the Internet as the mainstream perceives does not entirely represent what the entity is. Because of an increasing number of static HyperText Markup Language (HTML) pages, there is an enormous amount of information hidden in the layers of deep and dark Web where most search engines cannot have access (see Figure no. 2). The pathway to these remote Web locations is provided through static Uniform Resource Locator (URL) links due to their existence being depended on responses to queries submitted through the query interface of an underlying database. It is estimated that 43,000 to 96,000 deep Web sites exist along with 7,500 terabytes of data (He, Patel, Zhang & Chang, 2007).

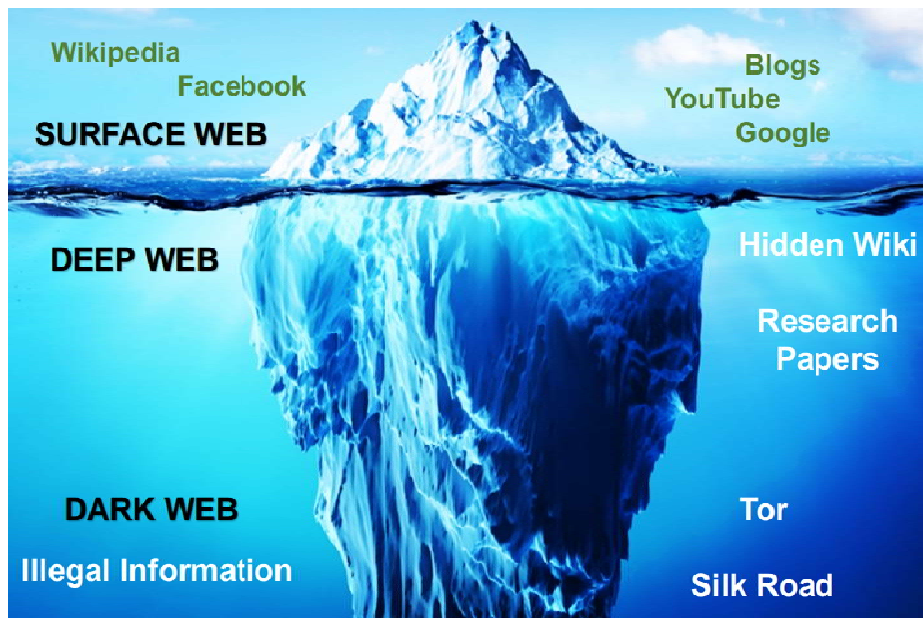


Figure no. 2: *Complete Web*

The issue with trying to locate deep websites is that they do not exist. That being the site is not indexed in a traditional sense like a standard search engine works. Take the search engine Google.com for example items are added to Google's database by either the website itself informing Google of their URL or the web crawlers looking for, finding, and indexing all "known" websites it finds. A deep website is not indexed in either capacity you need to know the URL of what you are searching for directly. Now there are

extensive databases that try to compile large amounts of search engine data, and these are called metasearch engines like DuckDuckGo (see Figure no. 3) and DogPile for example. These meta search engines allow you to search various standard search engines all at one time. In some cases, as many as 40-50 search engines can be searched with the entry of search terms and the press of a button. However, even these metasearch engines do not take into account the vast information that is found on the deep web.

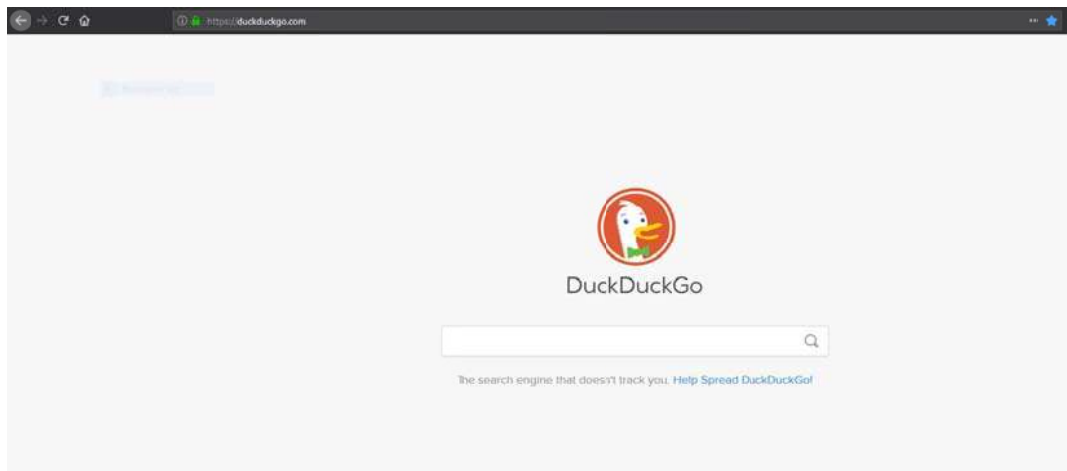


Figure no. 3: *Example of the DuckDuckGo Search Page*

There are several specialty search engines such as TORCH and the Onion URL Repository which index as many deep websites that can be found. The key to these types of search engines is that they do not act like traditional searches. You need to have access to TOR networks which work as a semi-autonomous network that provides private browser and viewing of sites. Once you are on this network, you still be able to access repositories of different search engines usually broken down by subject matter and start you dig into the deep web.

Another item of note is the deep web, and the dark web is not the same thing. While you may make use of TOR to access the dark web search engines that index the deep web. Both these environments are independent of each other. Deep websites sites can be found using traditional browsing methods as long as you know the URL for it where dark websites

leverage a software package like TOR to access the pages.

The Onion Router (TOR) gained popularity when the news was released around the globe about Edward Snowden exposing what the American government was doing with citizens' data. The tool of choice used was TOR. The Tor Browser can be used on Gnu Not Unix (GNU) Linux, Windows, and Mac without the need for installation of any software (Tor Project, n.d.). Tor was developed further by the Defense Advanced Research Projects Agency (DARPA) after the first principle of onion routing developed from a United States Naval Research Laboratory scientist. In Figure no. 4 shown are two Tor Browsers on Ubuntu Linux. The other browser shows The Uncensored Hidden Wiki and some onion links that have been verified. The first browser window displays the welcome message for anonymous exploration.

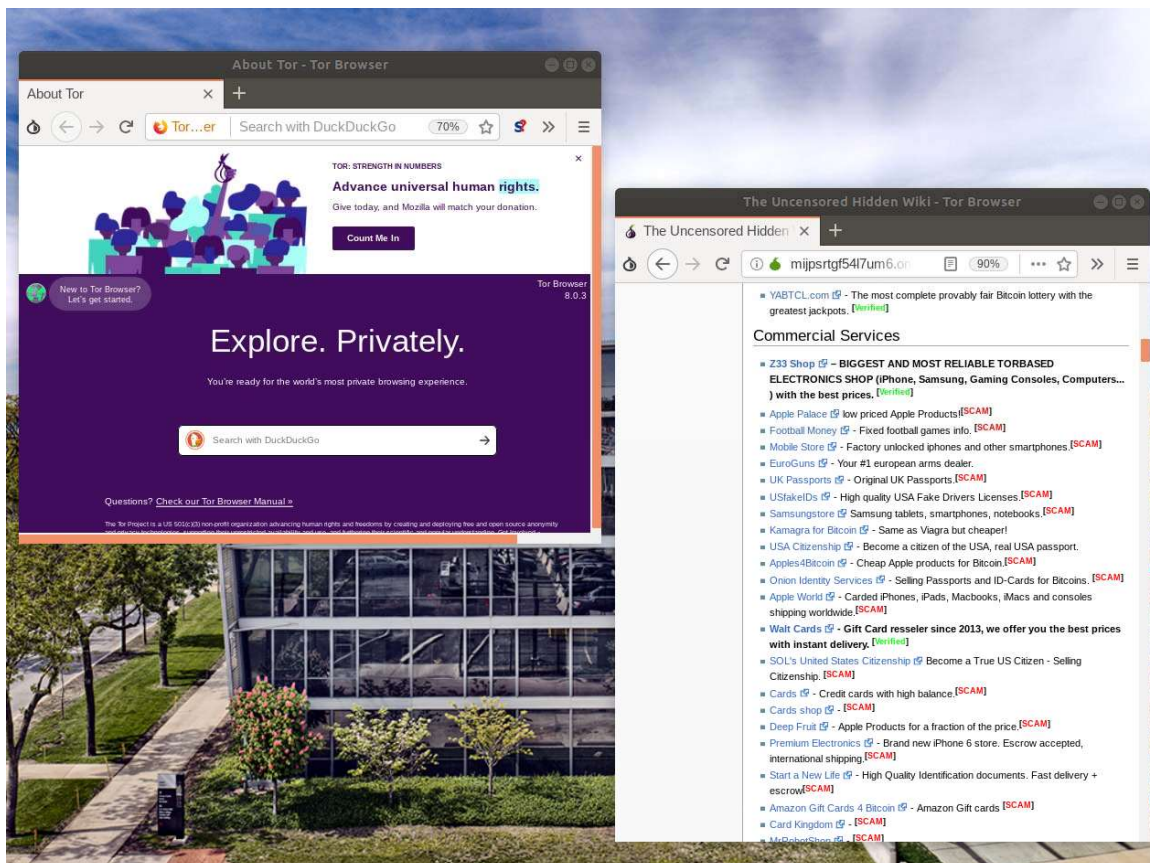


Figure no. 4: TOR Browsers

TOR is native in the Tails Operating Systems (OS) Tails is a Debian based Linux distribution which primary goal is the preserve privacy and anonymity to beat surveillance.

In recent years, organizations such as the NSA have been attacks this browser. One attack revealed was the exploitation of the Tor Browser Bundle. When using the Tor Browser security that leaves a system vulnerable such as Flash become enabled in this attack (Schneier, 2013). This attack targeted the Firefox browser by identifying the Tor Users and executing attacks against the browser (Schneier, 2013). Other tools detected Hypertext Transfer Protocol (HTTP) through Capability Network Exploitation (CNE), which is the starting point for finding Tor users. Researchers at the University of Waterloo and Stony Brook University discuss active attacks for website fingerprinting to identify destination web pages by passively observing their communication traffic (Wang, Nithyanand, Johnson & Goldberg, 2014).

However, these attacks have not deterred the use of Tor Browser. For users conducting illicit activities, this browser allows for undetected movement. One needs not to look too far to see the activities that occur on the Dark Web from the sale of illicit narcotics to human trafficking. Services from experienced hackers to assassins can be located using Tor and exploring Hidden Wiki.

Some browsers allow the user to protect their privacy. One such browser is Searx that does not share the users' IP, search history, and aggregates the results of more than seventy search engines (Tauber, n.d.). Searx browsers allow for advertisement filtering, personalization, and use of HTTP POST by default. Figure no. 5 shows the results of a search of Illinois Institute of Technology that populates that allows for files to be downloaded; pages scraped and allowed customization in terms of time.

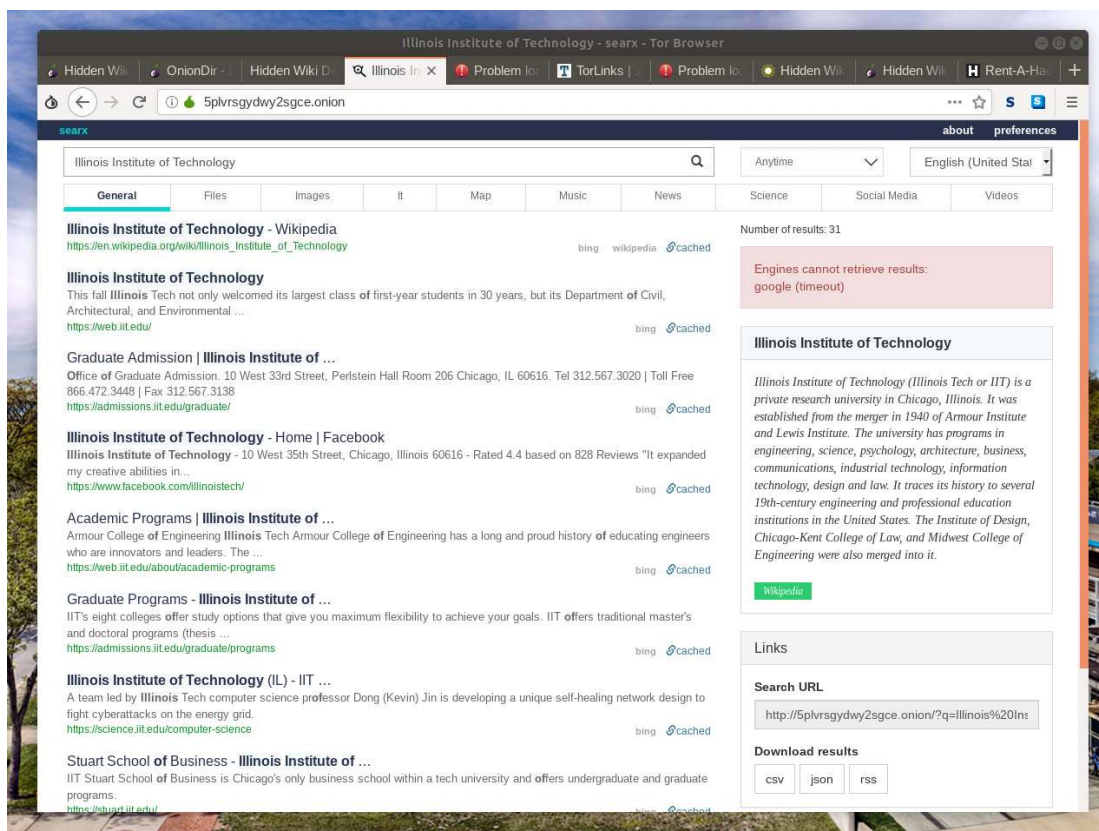


Figure no. 5: Searx Browser

There have been several occasions where the Tor network has been abused for personal gain. In 2013 a Harvard University student used this mean of anonymity to send emails to the school for a hidden bomb threat to avoid a final exam (Lin, Tong, Zhijie & Zhen, 2017). Silk Road is an online black market being accessed by nearly one million users through the exclusive access of the Onion Router. It includes illegal services like drug trafficking, child pornography, and arms trafficking; the value of its transactions has been calculated to be worth \$12 billion. Its operations were shut down in October 2013 by the Federal Bureau of Investigation (Lin, Tong, Zhijie & Zhen, 2017). “Anonymous” the notorious worldwide hacker organization, launched a DDoS attack against Sony Corp in April 2011. They used the anonymous network and managed to steal the personal data of nearly 1 billion people. This attack had a disruptive financial impact of \$171 million (Lin, Tong, Zhijie & Zhen, 2017).

6. Using Web for Targeted Warfare

Researchers have discovered that Internet sites such as YouTube Kids and YouTube have detected unsafe content through nefarious promoters that target kids through psychological means (Kaushal, Saha, Bajaj & Kumaraguru, 2016). This means that the threat landscape is altering to include all active users regardless of age or other constraints previously considered off limits. In the past mainly adults have been the targets of individuals or nation states however due to technological

advances and increased connectivity any connected user can be a target.

Reviewing the Open Web Application Security Project (OWASP) top 10 over the last ten years, it is apparent that the same critical web application vulnerabilities are still found (Wichers, 2013). One such vulnerability is the Common Weakness Enumeration (CWE) 89: Structured Query Language (SQL) Injection, which is rather easy to exploit using an application called sqlmap. A simple search of `php?id=[number]` while bringing up several websites through a query that can be a potential target.

7. Conclusion

The misuse of data and deficiency of knowledge to apply security controls is a critical issue across enterprise networks. The Internet has allowed for older techniques used for warfare to be modernized at levels that make a novice intelligence analyst near a Subject Matter Expert (SME). This is a drastic change to the landscape of the current battlefield in which is still evolving with the ever expansion of networked systems such as the Internet of Things (IoT) and 5G. The apparent scarcity of applied cybersecurity protections is allowing for threat agents to take advantage of organizations and individuals that lack the necessary knowledge for ensuring protection. This, combined with laws that do not require companies to have stronger security, enable attackers to perform exploits continuously.

REFERENCES

- Ahmed, S. R. (2004). Applications of data mining in retail business. *International Conference on Information Technology: Coding and Computing. Proceedings. ITCC, Vol. 2*, 455-459. IEEE.
- Aldrich, R. W. (1996). *The international legal implications of information warfare* (No. INSS-OP-9). Colorado: Air Force Academy Colorado Springs Co.

Aura, T., Kuhn, T. A., & Roe, M. (2006). Scanning electronic documents for personally identifiable information. *Proceedings of the 5th ACM workshop on Privacy in electronic society*, 41-50, New York, USA: ACM.

Boyd, D. M., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, Vol. 13, Issue 1, 210-230.

Chen, D., & Zhao, H. (2012). Data security and privacy protection issues in cloud computing. *International Conference on Computer Science and Electronics Engineering*, Vol. 1, 647-651, IEEE.

Clifton, C., & Marks, D. (1996). Security and privacy implications of data mining. *ACM SIGMOD Workshop on Research Issues on Data Mining and Knowledge Discovery*, 15-19.

Elbirt, A. J. (2003). Information Warfare: Are you at risk?. *IEEE Technology and Society Magazine*, Vol. 22, Issue 4, 13-19.

Elmasri, R. (2008). *Fundamentals of database systems*. India: Pearson Education.

Fussell, S. (2018). *Facebook's New Face Recognition Features: What We Do (and Don't) Know [Updated]*, available at: <https://gizmodo.com/facebook-new-face-recognition-features-what-we-do-an-1823359911>, accessed on 18 March 2019.

Gajanayake, R., Iannella, R., & Sahama, T. (2011). Sharing with care: An information accountability perspective. *IEEE Internet Computing*, Vol. 15, Issue 4, 31-38.

Gantz, J., & Reinsel, D. (2011). Extracting value from chaos. *IDC iview*, 1142, 1-12.

Gundecha, P., Barbier, G., & Liu, H. (2011). Exploiting vulnerability to secure user privacy on a social networking site. *Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining*, 511-519, New York, USA: Association for Computing Machinery.

He, B., Patel, M., Zhang, Z., & Chang, K. C-C. (2007). Accessing the deep Web. *Communications of the ACM*, 50(5), 94-101.

Headquarters Department of the Army (1979). Psychological Operations. *Field Manual*, No. 33-1, Washington: U.S. Government printing office.

Kaushal, R., Saha, S., Bajaj, P., & Kumaraguru, P. (2016). KidsTube: Detection, characterization and analysis of child unsafe content & promoters on YouTube. *14th Annual Conference on Privacy, Security and Trust (PST)*, 157-164, IEEE.

Krishnamurthy, B., & Wills, C. E. (2009). On the leakage of personally identifiable information via online social networks. *Proceedings of the 2nd ACM workshop on Online social networks*, 7-12, ACM.

Lin, Z., Tong, L., Zhijie, M., & Zhen, L. (2017). Research on Cyber Crime Threats and Countermeasures about Tor Anonymous Network Based on Meek Confusion Plug-in. *International Conference on Robots & Intelligent System (ICRIS)*, Vol. 1, 246-249, doi:10.1109/icris.2017.69.

O'Gorman, G., & McDonald, G. (2012). *Ransomware: A Growing Menace*, available at: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ransomware-a-growing-menace.pdf, accessed on 17 September 2019.

Schawartau, W. (1997). What Exactly is Information Warfare? – Part 2, *Journal Network Security*, Issue 10, Amsterdam: Elsevier Science Publishers.

Schneier, B. (2013). *Carry On: Sound Advice from Schneier on Security*, New Jersey, USA: John Wiley & Sons.

Sinisi, J. P. (2007). *U.S. Patent No. 7,313,759*, Washington, DC: U.S. Patent and Trademark Office.

Soma, J. T., Courson, J. Z., & Cadkin, J. (2009). Corporate Privacy Trend: The “Value” of Personally Identifiable Information (“PII”) Equals the “Value” of Financial Assets. *Richmond Journal of Law & Technology*, Vol. 15, Issue 4, 11.

Stalder, F., & Hirsh, J. (2002). Open source intelligence. *First Monday*, Vol. 7, Issue 6, 1-8.

Symantec Corporation. (n.d.). *What Are Cookies?*, available at: <https://us.norton.com/internetsecurity-how-to-what-are-cookies.html>, accessed on 07 July 2019.

Tauber, A. (n.d.). *Welcome to searx*, available at: <https://asciimoo.github.io/searx/>, accessed on 03 December 2018.

Tor Project. (n.d.). *What is Tor Browser?*, available at: <https://www.torproject.org/projects/torbrowser.html.en>, accessed on 03 December 2018.

Wang, T., Cai, C., Nithyanand, R., Johnson, R., & Goldberg, I. (2014). Effective Attacks and Provable Defenses for Website Fingerprinting. *The Proceedings of the 23rd USENIX Security Symposium*, San Diego, CA.

Wang, P., Dawson, M., & Williams, K. L. (2018). Improving Cyber Defense Education through National Standard Alignment: Case Studies. *International Journal of Hyperconnectivity and the Internet of Things (IJHIoT)*, Vol. 2, Issue 1, 12-28.

Wichers, D. (2013). *The Open Web Application Security Project (OWASP) Top10 -2013*. OWASP Foundation.