The University of Texas at Austin
Center for Identity

Proactive Identity Knowledge and Mitigation System

Aditya Tiaga
Razieh Nokhbeh Zaeem
K. Suzanne Barber

UTCID Report #21-10

December 2021

Abstract

While many organizations share threat intelligence, there is still a lack of actionable data for organizations to proactively and effectively respond to emerging identity threats to mitigate a wide range of crimes. There currently exists no solution for organizations to access current trends and intelligence to understand emerging threats and how to appropriately respond to them. This research project delivers I-WARN, to help bridge that gap. Using a wide range of open-source information, I-WARN gathers, analyzes, and reports on threats related to the theft, fraud, and abuse of Personal Identifiable Information (PII). Then maps those threats to the MITRE ATT&CK – a framework that helps understand lateral movement of an attack – to offer mitigation and risk reduction tactics. I-WARN aims to deliver actionable intelligence, offering early warning into threat behaviors, and mitigation responses. This paper discusses the technical details of I-WARN, current solutions for threat intelligence sharing with how they compare to I-WARN, and future work.

Proactive Identity Knowledge and Mitigation System

Aditya Tyagi[1], Razieh Nokhbeh Zaeem[2], and K Suzanne Barber[3]

[1]The University of Texas at Austin. email: adityatyagi6498@utexas.edu
[2]The University of Texas at Austin. email: razieh@identity.utexas.edu
[1]The University of Texas at Austin. email: sbarber@identity.utexas.edu

November 12, 2021

1 Introduction

With the world getting smaller through growing cyberspace, being connected with someone on the other side of the globe has never been easier. Unfortunately, that connectedness is used as an exploit. Digital footprints are becoming more exposed to the public; individuals and organizations are encouraged to understand the risk of exposure their *identity*-related actions hold. While many organizations share various types of threat intelligence, there is still a lack of actionable data for organizations to proactively and effectively access, understand, and respond to emerging *identity* threats to mitigate a wide range of crimes.

In this work, we created a new system named I-WARN. I-WARN offers timely identity threat information sharing and delivers timely actionable intelligence for decision-makers by leveraging a wealth of information and expertise found in the University of Texas Center for Identity's (UT CID) Identity Threat Assessment and Prediction (ITAP) [13], the MITRE ATT&CK framework and a wide range of open sources. Our novel **contribution**, in this work, is the creation of a system that is able to use Open Source Intelligence to create actionable data to take proactive mitigation actions against a threat. The system is designed to be publicly available and help organizations to defend against cyber incidents through added Threat Intelligence.

1.1 Threat Intelligence Context

Threat Intelligence enables individuals and organizations take a preemptive approach to their cybersecurity defenses as the newfound knowledge arms them with the ability to prioritize defending against attacks, should an attacker take any action against them. Threat Intelligence empowers the defending organization by introducing them to new vectors of attack, the attackers' patterns, motives as well as technical knowledge, and enabling them to make better decisions about prioritizations and risk mitigation tactics. Threat Intelligence, in current industry practice, falls under three categories: Strategic, Tactical, and Operational[1]. Strategic Intelligence ensures organizations and business understand the executive-level decisions that need to be made based on high-level analysis. Most sources for such intelligence are through open-source inputs, for example, media outlets, online reports, etc. Tactical Intelligence is more granular than high-level analysis as it serves to make technical decisions about the organization's defending systems and whether they can deter the immediate threats. Such intelligence takes inputs from IOCs: Indicators of Compromise consist of technical, forensic evidence which could indicate an attack or infection [21]. Further, Operational Intelligence answers the immediate questions of who is affected, how are they affected, and what is being used. This intelligence is often utilized to understand the context on various factors such as motivation, attack vectors, and other patterns.

1.2 Information Sharing and Opportunities from it

There has been industry exploration for improving cyber security information sharing. With the rise of digital dependency of the current US infrastructure, and the risks they can present[2], the US government had to further facilitate knowledge transfer through incentivized voluntarily information exchange. Under the Obama Administration, the Cybersecurity Information Sharing Act of 2015 was passed to further this agenda. With the law in place, federal government assures more protections to the private industry in exchange for sharing their threat indicators – technical knowledge such as IOCs – and their implemented defensive measures.

Through such encouragement of knowledge and intelligence sharing, non-profit organizations such as MITRE have stepped up to take advantage of the federal funding and partnerships between the public and private industries to ensure that such partnerships, through open sharing of such intelligence, aids in safer cyber-space of industries and nations[3]. MITRE has implemented a matrix – the ATT&CK Matrix – suggesting lists of possible horizontal movement throughout the incident response for any given cyber incident [14]. It should be noted that the United States CISA (Cybersecurity and Infrastructure Security Agency) alerts currently apply the MITRE mitigation and detection techniques, indicating the matrix is being actively used in private and public sectors as guidelines for incident responses.

With a rise of information sharing between private market sectors and the federal sectors, we have seen a surge in information provided through

[1] securityscorecard.com/blog/what-is-cyber-threat-intelligence-3-types-and-examples

[2] https://www.hoover.org/research/strengths-become-vulnerabilities

[3] www.mitre.org/about/corporate-overview

journalism and other media outlets. This information is conventionally classified as Open-Source Intelligence (OSINT): information which is available publicly and is encouraged to be used and shared for the betterment of the cyber communities. There are multiple types of OSINT outlets, and for the purposes of this research, we are focusing on the media outlets. Although OSINT – especially from media – is very effective as part of knowledge sharing, one of the severe limitations we see is the lack of technical details due to the jargon it introduces, inhibiting regular readers from understanding the context. This, in turn, results in less technical details for defending teams when parsing through the OSINT. The University of Texas's Center for Identity has utilized such open-source intelligence and created the Identity Threat Assessment and Prediction (ITAP) Model [13]. Though not actionable data, ITAP model aims to visualize the patterns and a higher-level analysis by providing Strategic Intelligence and extract vital information from the different stories.

2 Related Work

There has been previous academic work in the blue team sectors that focuses on helping market sector leads understand the different trends and cyber incidents. Although most of the resources discussed in the section covers work within the United States, some notable related efforts from the globe are acknowledged.

2.1 Information Sharing outside of United States

The Australian Cyber Security Centre (ACSC) issues surveys on annual basis that sends out aggregated information about the types, frequency, and impact of reported cyber incidents[4]. Although the report is extremely comprehensive which also includes incidents from different types of OSINT outlets and the type of impact faced by the incident, it fails to provide any data to encourage vigilance for specific market sectors.

On a global collaborative scale, The North Atlantic Treaty Organization (NATO) has attempted to share educational information about the different frameworks as well as possible mitigations from different attack vectors [12]. NATO shares their educational framework for the purposes of facilitating skill-based information for cyber-security professional all over the world. Since NATO does not entail or cater to one specific nation, the organization does not provide any data on any incidents that pertain to any nation.

2.2 Within United States

The Federal Bureau of Investigation's (FBI) Cyber Investigation team works closely with local law enforcement in its field offices. With the given coverage, individuals can request aid for incidents through FBI's Internet

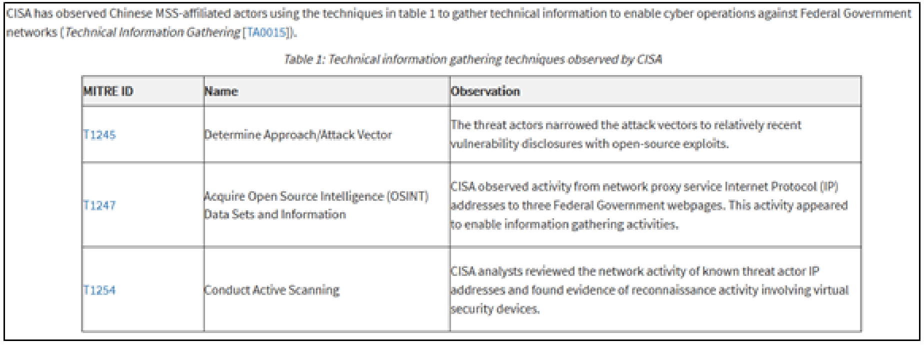
[4] `https://www.cyber.gov.au/sites/default/files/2019-03/ACSC_Cyber_Security_Survey_2016.pdf`

Crime Complaint Center (IC3)[5] while organizations can contact law enforcement and federal agents as need be. The Bureau releases certain attributes of the reported incidents such as basic demographic information, estimated financial impact, and types of cybercrimes that occurred. However, like other cyber security centers around the globe, the reports do not provide any mitigation responses as well as market sector specific trends that could indicate patterns for industry leads as they parse through the reports.

Additionally, US Department of Justice also aids in releasing reports to address the different cybercrimes trends and statistics, through the Bureau of Justice Statistics (BJS)[17] in aiding the US populace understand the different demographics of the victims involved in such crimes. However, the intention of such reports is to inform the public of annual trends and not to make any decisions. The reports provide a general cause of these cyber and information crimes, such as lack of anti-virus software, and derive the percentage of incidents caused by it. However, they do not provide any recommendation – implicit or explicit – to deter such attacks as a member of any organization or individual.

The Cybersecurity and Infrastructure Security Agency (CISA) provides time-sensitive and actionable alerts for the general public as well as the organizations to view and digest as they see fit[6]. CISA alerts follow the MITRE ATT&CK Framework analysis (discussed in the previous section) that ensures that mitigation response as well as detection techniques are easily understandable due to easy access to the framework. Figure 1 depicts one of the recent alerts with the ATT&CK Framework utilization. Although the alerts pushed by CISA are of industry and organizational interests, the agency does not use openly available information that pertains to incidents to domestic and local cyber incidents. With the federal government focusing on incidents that are of national security interest, actionable alerts would not cover domestic incidents such as social engineering or small ransomware cases as compared to local media.

Figure 1: A snippet of the CISA Alert AA20-258A showing MITRE ATT&CK implementation.



CISA has observed Chinese MSS-affiliated actors using the techniques in table 1 to gather technical information to enable cyber operations against Federal Government networks (*Technical Information Gathering* [TA0015]).

Table 1: Technical information gathering techniques observed by CISA

MITRE ID	Name	Observation
T1245	Determine Approach/Attack Vector	The threat actors narrowed the attack vectors to relatively recent vulnerability disclosures with open-source exploits.
T1247	Acquire Open Source Intelligence (OSINT) Data Sets and Information	CISA observed activity from network proxy service Internet Protocol (IP) addresses to three Federal Government webpages. This activity appeared to enable information gathering activities.
T1254	Conduct Active Scanning	CISA analysts reviewed the network activity of known threat actor IP addresses and found evidence of reconnaissance activity involving virtual security devices.

[5] www.ic3.gov

[6] us-cert.cisa.gov/ncas/alerts

2.3 Within United States: Academic and Industry work in Information Sharing

There has been academic exploration on how to integrate the ATT&CK Framework when supplying IOCs and its related information. From technical viewpoints, Farooq and Otaibi [7] depict multiple examples of utilizing machine learning (ML) and associating ML use cases with the ATT&CK Framework, notably for the Exfiltration detection techniques. The authors present K-Means clusters and relate them to a quadrant that is based off the Exfiltration techniques to detect user activity and any potential signs for malicious software injections or data leakage in forms of Command and Control, covert channels, etc. The work provides detail in mimicking the detection techniques for any organization's SOC although it does not provide any testing criteria or compare accuracies from open databases. However, such information sharing on detection is exceptionally important to integrate with industry standards of attack techniques and behavior because of the novel cases seen by organizations, enabling their SOCs to detect IOCs attacking their organization.

The University of Texas's ITAP reports[7] utilize news stories and other open-source information gathering outlets to collect information about PII related cyber incidents. The ITAP model can capture high amounts of incidents as raw data and parse through to understand the vulnerabilities exploited, data that was breached, and steps taken by the bad actor to achieve the goal. It accounts for cases after the year 2000 and can analyze trends in the types of cyber incidents as well as the market sector. The report further details the findings and visualizes it into different categories and trends such as impact of loss, demographics of victims, etc. ITAP Model has set precedence in understand how PII is exploited and the key identity assets that are used for the exploit. Various other academic works use the ITAP Dataset to further research the PII assets, their risk of exposure, protection strategies, and minimizing risk [3, 18, 1, 10, 15, 6, 9, 8, 16, 2, 19, 11, 4, 5].Though it aids in visualizing the trends and patterns of cyber incidents in various market sectors, it fails to provide the information in a timely manner that can be incorporated by individuals and organizations alike and attempt to take any preventive actions to protect themselves from the attack. Moreover, with the given information, ITAP is not able to provide any explicit recommendations for prevention measures.

Like ITAP, Verizon releases data breach reports with incidents that are related to its forensic and intelligence operations[8]. The incidents that are explained in the annual report are shaped in the VERIS Framework[9] – which is similar to the ATT&CK Framework as described above – that standardizes the information extracted. Verizon's report is very comprehensive because it can capture concrete steps, threat patterns, frequency, and the data compromised. The report, based on the trends and other factors, releases general recommendations for security effort but does not

[7] identity.utexas.edu/sites/default/files/2020-09/ITAP_Report_2018.pdf

[8] enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

[9] veriscommunity.net

give any recommendation at an individual incident basis or even market sector basis.

There is a plethora of companies that attack this domain issue of threat intelligence in forms of business models. Companies such as Crowdstrike[10], IBM X-Force[11], Virustotal[12], etc. have business models oriented towards gathering threat intelligence in all formats followed by digesting, analyzing, and reporting the information in timely manner to the organization. With the current subscription costs of such services being closer to ten thousand dollars per annum, smaller organizations can get isolated as they likely do not have the same budgets for cybersecurity as bigger organizations. Further, the budgeting of smaller enterprises tends to focus more on endpoint protection for reactive response rather than intelligence gathering for a proactive approach, as advised by the framework put out by CISA[13], leading to intelligence gathering be of lower priority and risk smaller organizations be a lucrative target for bad actors.

3 System Overview

I-WARN is designed to be a webpage that can be accessed by any device connected to the internet. We use Python 3.7 for the backend logic, ITAP dataset to digest the inputs, and Python Flask[14] coupled with HTML and JavaScript for the front end. More aspects of each part of the project are detailed below.

On a high-level overview, The ITAP dataset is fed into a parser script where it is parsed to extract information elements, such as steps or inputs used by attackers during an incident, for the system to map a story to a specified ATT&CK threat tactic from the matrix through a scoring system. We discuss why we used ATT&CK matrix later. Once the information is collected, we create a score for each story to understand the more likely threat tactic utilized based on the inputs and steps taken by the attacker during an incident. Lastly, when the scores are created, we further extract the market sector and send over the details to an automation script for it to create a possible list of mitigation tactics. From there, the output is then fed into the Graphical User Interface (GUI) where it can display descriptions, mitigation tactics, and top threat tactics for each story. There are other features such as the CISA Alert feed also available from the GUI. Figure 2 gives a high-level overview of the whole system to further visualize I-WARN.

3.1 ITAP Dataset

We utilize the ITAP dataset from previous work [13, 20]. Table 1 shows a snippet of the information contained for each story. We created the backend with the dataset because of the thoroughness and versatility it

[10] www.crowdstrike.com/products/threat-intelligence/falcon-x-recon

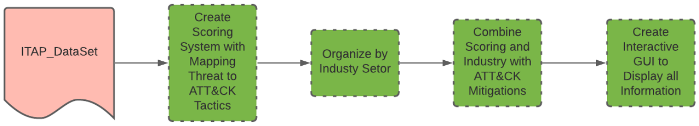
[11] exchange.xforce.ibmcloud.com

[12] www.virustotal.com/gui/home

[13] us-cert.cisa.gov/resources/cybersecurity-framework

[14] github.com/pallets/flask

Figure 2: Overview of I-WARN: the lifecycle of each story from the ITAP dataset to the frontend.


ITAP_DataSet
Create Scoring System with Mapping Threat to ATT&CK Tactics
Organize by Industy Setor
Combine Scoring and Industry with ATT&CK Mitigations
Create Interactive GUI to Display all Information

Inputs	Outputs	Steps	Loss Incurred
Malware Injected	Personally Identifiable Information (PII)	Breach,Infect,Acquire	Emotional Distress
Victim(s) Selected	DDoS Attack Initiated	Coordinate,Act Upon	Financial, Property, Reputation
File(s) Copied without Authorization	Organization Proprietary Information	Transfer, Steal	Intellectual Property

Table 1: A snippet of the ITAP dataset with inputs, outputs, and steps taken by the bad actor. Information contained in the table for each story is not exhaustive.

provides. The different sources of OSINT ITAP utilized gives the diversity of gathering intelligence from all over the publicly available outlets. Further, each story is manually parsed through to get the most information out of it and is divided into the appropriate column. From inputs used by the attacking actor to the impact on victim, each story's facts are captured and condensed into the dataset. Gathering of all the information indicates a very thorough study of each story and reaffirms every piece of intelligence which can be extracted. Currently, the ITAP dataset contains approximately 6000 stories gathered from the OSINT outlets, captured between the years 2000 and 2020. These stories are manually modeled but efforts are underway to fully automated modeling with machine learning [13]. Most of the stories contained in the dataset are related to identity-related crimes such as identity theft, social engineering, and phishing.

3.2 Backend Works

We start the discussion of backend logic with the utilization of MITRE ATT&CK Framework[15]. Currently, ATT&CK framework is being utilized by actionable alerts provided by CISA[16] as well as by multiple non-federal information sharing[7, 22]. The framework incorporates previous history of possible attacks and attributional details. Further, it lists out possible detections and mitigations with each tactic and technique to help understand what are the best courses of actions that can be taken for a proactive or reactive defense for such attacks. With such eclectic set of information provided – and regularly updated – as part of OSINT, it was easier for us to integrate the framework in our work. Next, we designed a logic map based on the keywords used in the ITAP dataset. The inputs and steps used in each story, as described in Table 1, give an overall picture about the incident that has taken place. Since there are stories generalized, we

[15] attack.mitre.org

[16] us-cert.cisa.gov/ncas/alerts

Tactics	**ITAP Input used**	**ITAP Steps used**
Reconnaissance	“Broken Into”,“Phishing”,“Social Media”	“Analyze”,“Surveil”,“Break Into”,“Misplace”,“Mismanage”
Resource Development	”Compile”,”Lie”,”Communicate”,”Alter”	”Impersonate”,”Compile”,”Lie”
Initial Access	”Security vulnerability/Mismanage”,”Phishing/Spear-Phishing”,”PII/Credential Stolen”	”Request”, ”Send”, ”Infect”
Execution	”Malicious Link”,”Malware”,”Ransomware”	”Breach””
Persistence	”Access Misuse”	”Abuse”,”Create”,”Activate”
Privilege Escalation	”Access Misuse”	”Abuse”
Defense Evasion	”Access Misuse”	”Conceal”
Credential Access	”Security vulnerability/Mismanage”,”Devices Mishandled”	”Steal”,”Record”
Discovery	NONE	NONE
Lateral Movement	NONE	NONE
Collection	”Audio/Visual Involvement”,”Removable Media”,”Email Scam”	”Record”,”Discover”,”Find”
Command and Control	NONE	NONE
Exfiltration	”Removable Media”,”Transfer”	”Inflict Punitive Measure”,”Upload”,”Steal”
Impact	”Ransomware”,”DDOS”,”Video Altered”	”Disable”,”Destroy”,”Block”,”Deactivate”,”Send”,”Request”

Table 2: A snippet keywords from ITAP dataset used to create the scoring system.

decided to not attempt to narrow down on techniques but rather keep it broader with tactics to avoid any risk of overfitting the dataset. Table 2[17] shows us the manual logic used for mapping keywords to tactics in the framework.

To ensure keywords are captured correctly, we grouped many inputs to the proper keyword, reinforcing the logic as well as making it more simplistic when mapping to tactics. For example, we grouped inputs such as “Twitter”, “Facebook”, “social media” as Social Media Involvement. We collected and grouped all the ITAP inputs into 20 keywords, as shown in Table 2. Due the specification provided in the dataset, we further generalized the market sector to aid in understanding of general trends. For instance, we grouped together market sectors containing the keyword “health”, “hospital”, “clinics”, etc. as healthcare. We grouped together all the market sectors of 6000 stories into 12 market sectors. 11 out of 12 market sector keywords are readily mappable to known classification of market sectors, such as healthcare, religious organizations, etc. Out of the 11, 7 are classified to be part of the CISA Critical Infrastructure Sectors[18]. The remaining four are known sectors: education, religious organizations, hotels, and travel. The 12th one is meant of miscellaneous – market sectors and companies that are not well known or do not fit in a generic sector – such as anonymous organizations, various companies grouped, clubs, etc. We classify organizations as miscellaneous if they cannot be grouped into the 11 other classifications. This information is collected and then passed on to be viewed on the GUI. This separation of market sectors ensures that leaders of specified market sector can view generalized trends in their fields as well as explore the stories specific to their market sector. This would ensure they are able to filter out any noise related with other market sectors and take reactive or proactive measures based on the news, threat tactics, and mitigation suggestions.

Given the stories are manually parsed and have been fully extracted, some contents of stories lead to ambiguity when it comes to pinpointing the exact tactic utilized by the bad actor. To counter that, we created a scoring system which assists in pinpointing the “most likely” tactics used. We overlap a few keywords – as seen in Table 2 – and give them a likely score of the possible tactics used. This ensures we can create a coverage that is adaptable as more stories pour in, without risking to narrow results based on the specified 6000 stories.

[17] https://tinyurl.com/68nnyafr

[18] www.cisa.gov/critical-infrastructure-sectors

Since the ITAP dataset is comprised of OSINT from media outlets, all the technical details described in the framework cannot be mapped to the stories. To eliminate this issue, we created a dictionary to take out extremely technical techniques. We also eliminated sub-techniques that stemmed from the said techniques. This way, we are able to filter out mitigations that are not applicable to techniques which are never addressed in the dataset. This is one the limitations of this work which will be discussed in later sections. Furthermore, since each story extracts top three threat tactics used in the incident, and each threat tactic has a mitigation tactic list linked to it, we attach the lists of these mitigation tactics which are associated with the threat tactics. However, for brevity, we only display the list for top threat tactic in each story. Displayed mitigation tactics are then hyperlinked with the MITRE website and displayed for the reader.

Because the CISA alerts are published ready and integrated with the MITRE Framework, adding the alerts seemed like a vital feature to incorporate in I-WARN as it then offers itself as a hub to more intelligence – governmental and non-governmental alerts – that organizations can utilize from one location. As part of future works, we aim to expand and incorporate other open knowledge sharing systems as well. We use Flask for I-WARN due to the increased dependency of a web framework and the ease it offers to upload the project on platforms, like Amazon Web Services, when we are ready to publish. Figure 3 shows us the main homepage that a user would see whenever they go to the system. We see the tabs to each market sector, as well as CISA alerts, are readily available for the user to navigate to. Further, the homepage also has an interactive pie chart that shows the current number of cases for each market sector. The pie chart is created using HTML and embedded JavaScript through Google charts as well as other sources for navigation bars[19] and is adaptable to more market sectors, should they be added in the future.

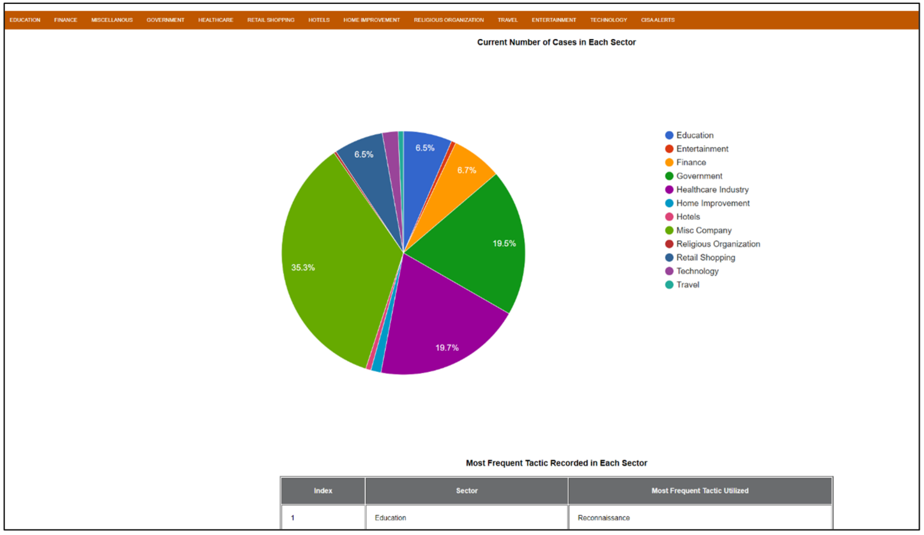
Diving deep into each sector, the stories are granulated into the story number – which is a simple index that can be replaced with more specific names – followed by the top 3 tactics likely used in the story. These tables, like the homepage, are interactive and can be clicked to get more information. We created a list in the backend and linked it to the MITRE website in case the reader wants more information about each mitigation and how it relates to different techniques. We also conducted a frequency analysis on all the mitigations and give a priority mitigation suggestion based on the mitigation which covers the most tactics used in each story.

4 System Comparison

To ensure that our system stands as a functional intelligence sharing platform, we observe different platforms that are advertised as knowledge sharing systems and compare them to I-WARN in terms of information content, ease of access, etc.

[19] developers.google.com/chart/interactive/docs/gallery/piechart

Figure 3: A snippet from the GUI: the web homepage, the pie chart showing the number of cases in each market sector, the education trends for tactics at the bottom.



Most Frequent Tactic Recorded in Each Sector

Index	Sector	Most Frequent Tactic Utilized
1	Education	Reconnaissance

4.1 Cybersecurity and Infrastructure Security Agency (CISA)

CISA, as described earlier, is the United States federal resource when alerting the public about cybersecurity incidents and related mitigation response. Through federal resources, they focus on incidents that are of national security interest as well as any incidents that target the Critical Infrastructures. CISA collaborates with multiple partners in the federal and private cyber watch sectors to collect information. As seen in Figure 1, CISA alerts regarding persistent threats that endanger Critical Infrastructure Services comprise of the background of the alert, detection, and mitigation responses – all of which are extracted from the MITRE framework. Comparing the CISA alerts to Figure 3, we see that I-WARN derives all its information sharing content from the CISA alerts. Because each story is extracted from media outlets, I-WARN does not concern itself with given explicit background on each story under the assumption that an extensive coverage of the story has already been done. We plan on adding hyperlinks to each story as part of our future work. Looking at detection and mitigation tactics, I-WARN provides mitigation responses with the links to MITRE mitigation description for the reader to better understand how the mitigation tactic is integrated in their system. The links also serve as a bridge to further investigate what threat techniques are said to be mitigated from the recommendation. Because of the ease of access to the detection and mitigated techniques, I-WARN compares well with CISA alerts because of the content they both share. Any reader should be able to get in-depth information about cybersecurity alerts available through media outlets through I-WARN in similar fashion of alerts of national security interest through CISA.

4.2 Australian Cyber Security Centre (ACSC)

We look at the Australian Cyber Security Centre (ACSC) alerts[20] as they annually release white reports to ensure that their citizens and organizations understand cybersecurity trends and take general mitigation steps. We observe that ASCS – like CISA – releases a brief description about the cybersecurity alert as well as mitigation response. Although it does not directly relate to the MITRE framework, the mitigation responses are guidelines to review for Indicator of Compromises and recommendation to prevent the intrusion related to the system. It should also be noted that the alerts common for Australia and United States mimic the same mitigation responses and often the ASCS would recommend reading the CISA mitigations. Like ACSC, I-WARN ensures that the mitigation tactics are granular to each story and are hyperlinked to more details, so that they can be further understood by following the links.

4.3 Sources from Twitter

One of the most common information sharing platform which is not governed by a single entity or organization is Twitter. The social media is very versatile that can be used as part of OSINT as well as knowledge sharing platform. Various cybersecurity organizations send out tweets that are not as organized as the formal systems discussed previously but send out information about incidents in a timely manner. We observe The Hacker News as part of our informal knowledge sharing[21]. The Hacker News is very active on twitter in releasing information about cybersecurity events. The Hacker News covers a diverse range of incidents which do not necessarily overlap with any government alerts as seen on ASCS or CISA. Since The Hacker News have their own cybersecurity researchers and journalists, they are able to invest in resources to collect information for domestic and international incidents. However, as discussed before , the tweets are shared in high frequency which does not give enough time for The Hacker News or any other independent source to collect and analyze all the possible IOCs and give any mitigation recommendation. Although it is faster in delivery of intelligence, I-WARN contains more details about the stories that are posted in the system as compared to The Hacker News tweets [22]. Other informal sources posting information related to cybersecurity incidents and stories are independent sources and individuals that do not systematically hunt and post incidents. For instance, media outlets such as Wall Street Journal (@WSJCyber) would inform the public about cyber security incidents. However, their cyber news does not always cover incidents but also politics that involve cyber news. This unreliability makes such sources a weak comparison against

[20] `Cyber.gov.au`

[21] `thehackernews.com`

[22] Does not include retweets by The Hacker News from other organizations.

I-WARN due to its dedicated approach to share OSINT and mitigation recommendations.

4.4 Cyware

Other platforms that we compare I-WARN to are independent websites such as Cyware[23] that releases news about cybersecurity incidents and related policies. Cyware as a system is able to separate out news relating to incidents and policies, which makes it easier for the reader to access the content of their choosing. This compares well with I-WARN as it gives the user the abilities to choose the information they require from each sector. Further, since Cyware itself does not post the alerts but rather links and highlights the alerts from different websites, it is a fast delivery system that can be monitored at a high frequency for any updates. Since it links the readers to websites like The Hacker News, we see the same issue as described above: in the tradeoff for timely alerts, there is not enough information to analyze the IOCs for any detection or mitigation responses. Although websites like Cyware can deliver alerts and notifications faster than I-WARN, they do not have the same content to recommend any proactive or reactive actions for their readers.

5 Future Work

As we conclude our work, we highlight some plans for any future work.

5.1 Keeping The System Open-Source and Live

One of the near-future goals for I-WARN is to be live and accessible by public-facing internet. With the Python webhook developed, we are currently exploring options of Amazon Web Services (AWS) through Elastic Beanstalk due to its ease of pushing Python Flask webhooks. Through Beanstalk, we will be able to store the source code to an S3 bucket and have an open connection to the webpage through port 80. Although security and having HTTPS traffic is vital and in consideration, our priority is to have a live page first. We will continue to explore other options in the realm of AWS to bring the application up and usable for the public.

5.2 Collecting Information From More Sources

One of the planned, near future work for I-WARN is expanding the resource pool of OSINT gathered. Currently, I-WARN relies on information gather from various outlets for ITAP. Although it provides a versatile set of data for mitigation efforts to be displayed, we are hoping to expand to add more sources and increase the information flow for the ITAP dataset to work with. Higher globalization and interconnectivity results in being connected to one part of the world, while sitting in at the other side. Although this globalization makes the world a smaller place for people

[23] cyware.com/cyber-security-news-articles

to connect, unfortunately, it brings global threats to organizations or individuals' Homefront as well. We plan on incorporating news sources from all over the globe, such as 9news from Australia[24], Economic Times from India[25], etc. It would ensure preventive measures are recommended based on threats which are not just currently present in the US, but also all around the world. With a broader scale of events being digested by I-WARN, readers for any sector will be able to better picture the shape of their market sector on a global scale and prepare their cybersecurity measures accordingly. Not only will they be able to focus on threats already occurring in the US, but also be able to proactively prepare themselves, if their organization has any open communication or any relation with countries of interest based on the dataset. With the location in mind, I-WARN aims to distinguish source of the story in addition to the distinguished sectors, giving the reader a better idea of where the incidents are occurring and if investing in mitigation recommendations is necessary for them.

5.3 Using Machine Learning

The current ITAP dataset has been manually parsed to extract all the information from each story. Although the process is very thorough, it leaves room for errors due to subjectivity and is in general very crude and cumbersome. Similarly, I-WARN logic mapping is manually integrated, leaving room for the same issues. As part of future work, we plan on utilizing the upcoming machine learning models to train on the current ITAP dataset and logic such that keywords and inputs can be automatically extracted. With the addition of new sources, manually parsing through all stories will be rendered ineffective soon and use of ML is going to be imperative should ITAP and I-WARN keep digesting of new information on a very high frequency. The University of Texas's Center for Identity is currently working on using ML to automate all capturing of needed information for the ITAP dataset. With the models, I-WARN will be able to integrate new stories and update its dashboard on a higher frequency, as the new information is fed in. Further, we aim to work on ML models for I-WARN to be able to incorporate newer keywords and inputs as the stories add more detail. This will especially be useful when synonymous for various keywords – such as "medical centre" instead of "hospitals" – can be seen in use for news sources in other parts of the world. It would also aid in incorporating different inputs which can be used for different threat techniques and tactics as new vectors for attack surface. Using Machine Learning, we can streamline the process of parsing through incoming sources, collecting inputs and steps taken by the bad actor, as well as map them to specified threat tactic and techniques. It will aid in fully narrowing down the mitigation recommendations, leveraging the full power of OSINT and benefitting the communities.

[24] www.9news.com.au/cyber-security

[25] cio.economictimes.indiatimes.com/tag/cybersecurity

5.4 Incorporating all MITRE Techniques

One of the limitations discussed in previous sections was the elimination of several techniques that could not be mapped to any stories in ITAP due to the lack of technical context in the current media outlets. With the increasing interdependence of information sharing and growing interest of cyber and information security in public and private organizations, we hope that OSINT retrieved from media outlets will start to provide more context on the technical details of various cyber incidents. Through the technical insights, we would be able to incorporate the keywords retrieved into I-WARN's scoring system and provide narrowed mitigation efforts for the different techniques being utilized by the bad actors. Due to the required efforts of organizations which I-WARN relies on, we keep this as an attainable goal for distant future. The needed evolvement of OSINT will require fundamental changes on media's information sharing procedures, foreshadowing a long wait for the technical details to be shared in story. Regardless of the wait, it is an imperative work which needs to be incorporated whenever possible. As leaders in I-WARN's covered sectors, all information collected to provide mitigation can result in preventing their organizations suffer immeasurable or irreversible damage. The more techniques we cover, the better it is for defending organizations.

All in all, though I-WARN is a system that aids in turning OSINT into actionable intelligence, the system is far from perfect. With our step in the right direction, we hope to continue our work for the betterment of organizational defenses through gather more intelligence from around the globe, streamlining our pipelines from ITAP dataset to webpage using Machine Learning, using MITRE to its full ability, and bringing the system live for the world to view and use. These expectations would ensure that I-WARN is a relevant system when threat intelligence is discussed as a topic.

6 Conclusion

We delivered I-WARN, an actionable identity threat intelligence and analysis tool with recommendations to mitigate and thwart threats, leveraging the integration of open sources (e.g., news media), the UT Center for Identity Threat Assessment and Prediction (ITAP) project data, and the MITRE ATT&CK framework. I-WARN ensures leaders are better prepared for cyber threats observed in the community. Using ITAP dataset, I-WARN can utilize openly available information, such as inputs and steps used by attackers, to map them with the current ATT&CK framework that enables getting actionable data for readers and leaders of various market sectors. It is incredible to see how trivial information received from various media outlets, like blogposts and articles, can be turned in a power tool to better the defenses of organizations.

Threat Intelligence is one of the strongest tools a cyber-defending team has in its arsenal. In the battle between attackers and defenders, attackers bring the advantage of weaponizing new vulnerabilities that defenders must reactively respond to. With threat intelligence aiding the defenders to proactively know about a threat, we hope that I-WARN delivers a significant advantage to the defenders by increasing the actionable intelligence available for organizations and their leadership.

Declaration of Conflicting Interest

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

This work was in part funded by the Center for Identity's Strategic Partners. The complete list of Partners can be found at `https://identity.utexas.edu/strategic-partners`.

References

[1] Suzanne Barber. Identity threat assessment and prediction (itap) - keesing ..., Feb 2019.

[2] Kai Chih Chang, Razieh Nokhbeh Zaeem, and K. Suzanne Barber. Is your phone you? how privacy policies of mobile apps allow the use of your personally identifiable information. In *2020 Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, pages 256–262, 2020.

[3] Kai Chih Chang, Razieh N. Zaeem, and Suzanne K. Barber, Mar 2018.

[4] Kai Chih Chang, Razieh Nokhbeh Zaeem, and K. Suzanne Barber. Enhancing and evaluating identity privacy and authentication strength by utilizing the identity ecosystem. In *Proceedings of the 2018 Workshop on Privacy in the Electronic Society*, WPES'18, page 114–120, New York, NY, USA, 2018. Association for Computing Machinery.

[5] Kai Chih Chang, Razieh Nokhbeh Zaeem, and K. Suzanne Barber. A framework for estimating privacy risk scores of mobile apps. In Willy Susilo, Robert H. Deng, Fuchun Guo, Yannan Li, and Rolly Intan, editors, *Information Security*, pages 217–233, Cham, 2020. Springer International Publishing.

[6] Chia-Ju Chen, Razieh Nokhbeh Zaeem, and K. Suzanne Barber. Statistical analysis of identity risk of exposure and cost using the ecosystem of identity attributes. In *2019 European Intelligence and Security Informatics Conference (EISIC)*, pages 32–39, 2019.

[7] Hafiz M. Farooq and Naif M. Otaibi. Optimal machine learning algorithms for cyber threat detection. In *2018 UKSim-AMSS 20th International Conference on Computer Modelling and Simulation (UKSim)*, pages 32–37, 2018.

[8] Michael Kuperberg. Blockchain-based identity management: A survey from the enterprise and ecosystem perspective. *IEEE Transactions on Engineering Management*, 67(4):1008–1027, 2020.

[9] David Liau, Razieh Zaeem, and Suzanne Barber. An evaluation framework for future privacy protection systems: A dynamic identity ecosystem approach, Feb 2020.

[10] David Liau, Razieh Nokhbeh Zaeem, and K. Suzanne Barber. Evaluation framework for future privacy protection systems: A dynamic identity ecosystem approach. In *2019 17th International Conference on Privacy, Security and Trust (PST)*, pages 1–3, 2019.

[11] David Liau, Razieh Nokhbeh Zaeem, and K. Suzanne Barber. A survival game analysis to personal identity protection strategies. In *2020 Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, pages 209–217, 2020.

[12] NATO. Deep: Cybersecurity - a generic reference curriculum, Aug 2018.

[13] Razieh Nokhbeh Zaeem, Monisha Manoharan, Yongpeng Yang, and K. Suzanne Barber. Modeling and analysis of identity threat behaviors through text mining of identity theft stories. *Computers & Security*, 65:50–63, 2017.

[14] Adam Pennington, Andy Applebaum, Katie Nickels, Tim Schulz, Blake Storm, and John Wunder, 2019.

[15] Rima Rana, Razieh Nokhbeh Zaeem, and K. Suzanne Barber. Uscentric vs. international personally identifiable information: A comparison using the ut cid identity ecosystem. In *2018 International Carnahan Conference on Security Technology (ICCST)*, pages 1–5, 2018.

[16] Rima Rana, Razieh Nokhbeh Zaeem, and K. Suzanne Barber. An assessment of blockchain identity solutions: Minimizing risk and liability of authentication. In *2019 IEEE/WIC/ACM International Conference on Web Intelligence (WI)*, pages 26–33, 2019.

[17] Ramona R. Rantala. Cybercrime against businesses, 2005, Sep 2008.

[18] Razieh Nokhbeh Zaeem, Suratna Budalakoti, K. Suzanne Barber, Muhibur Rasheed, and Chandrajit Bajaj. Predicting and explaining identity risk, exposure and cost using the ecosystem of identity attributes. In *2016 IEEE International Carnahan Conference on Security Technology (ICCST)*, pages 1–8, 2016.

[19] Razieh Nokhbeh Zaeem, Monisha Manoharan, and K. Suzanne Barber. Risk kit: Highlighting vulnerable identity assets for specific age groups. In *2016 European Intelligence and Security Informatics Conference (EISIC)*, pages 32–38, 2016.

[20] Jim Zaiss, Razieh Nokhbeh Zaeem, and K Suzanne Barber. Identity threat assessment and prediction. *Journal of Consumer Affairs*, 53(1):58–70, 2019.

[21] Shengping Zhou, Zi Long, Lianzhi Tan, and Hao Guo. Automatic identification of indicators of compromise using neural-based sequence labelling, 2018.

[22] Polina Zilberman, Rami Puzis, Sunders Bruskin, Shai Shwarz, and Yuval Elovici. Sok: A survey of open-source threat emulators, 2020.

WWW.IDENTITY.UTEXAS.EDU