Electronic Communications of the EASST
Volume 080 (2021)

Conference on Networked Systems 2021 (NetSys 2021)

Early Warning Identity Threat and Mitigation System

Aditya Tyagi, Razieh Nokhbeh Zaeem, K. Suzanne Barber

4 pages

Guest Editors: Andreas Blenk, Mathias Fischer, Stefan Fischer, Horst Hellbrueck, Oliver Hohlfeld, Andreas Kassler, Koojana Kuladinithi, Winfried Lamersdorf, Olaf Landsiedel, Andreas Timm-Giel, Alexey Vinel
ECEASST Home Page: http://www.easst.org/eceasst/ ISSN 1863-2122

Early Warning Identity Threat and Mitigation System

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

The University of Texas at Austin

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 Personally Identifiable Information (PII). I-WARN 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, non-exhaustive current solutions for threat intelligence sharing, and future work.

Keywords: Information Security, Open Source Intelligence, Threat Intelligence

1 Introduction

Theft, fraud, and abuse of Personally Identifiable Information (PII) shared and collected online are on the rise. Individuals and organizations are encouraged to understand the risk of exposure their identity-related tokens hold. In this work, we created a new system named I-WARN. I-WARN offers timely 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) [NMYB17], 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.

2 Threat Intelligence through Information Sharing

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.

With a rise of information sharing between private market sectors and the federal sectors, we have seen a surge in information provided through 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. 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. The University of Texas's Center for Identity has utilized such open-source intel and created the Identity Threat Assessment and Prediction (ITAP) Model [NMYB17]. 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.

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[1] coupled with HTML and JavaScript for the front end. More aspects of each part of the project are summarizded below.

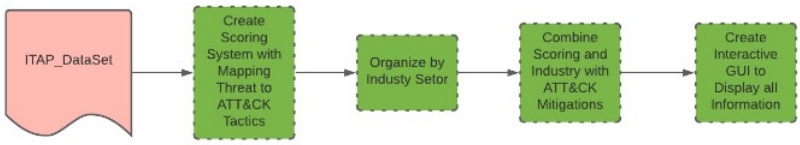
On a high-level overview, The ITAP dataset is fed into a parser script where it is parsed to extract information elements, such as steps or inputs used by attackers during an incident, for the system to map a story to a specified ATT&CK threat tactic from the matrix through a scoring system. Currently, ATT&CK framework is being utilized by actionable alerts provided by CISA[2] as well as by multiple non-federal information sharing[FO18]. 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.

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 1 gives a high-level overview of the whole system to further visualize I-WARN.

We utilize the ITAP dataset from previous work [NMYB17, ZNB19, ZMB16]. 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 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

[1] github.com/pallets/flask
[2] us-cert.cisa.gov/ncas/alerts

Figure 1: Overview of I-WARN: the lifecycle of each story from the ITAP dataset to the frontend.



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.

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 [NMYB17]. Most of the stories contained in the dataset are related to identity-related crimes such as identity theft, social engineering, and phishing.

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.

We use Flask for I-WARN GUI 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.

4 Future Work

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. Secondly, we plan on incorporating news sources from all over the globe, which would ensure preventive measures are recommended based on threats which are not just currently present in the US, but also all around the world.

The current ITAP dataset has been manually parsed to extract all the information from each story. As part of future work, we plan on utilizing the upcoming machine learning models to train on the current 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. 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 tactic and techniques.

5 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.

Bibliography

[FO18] H. M. Farooq, N. M. Otaibi. Optimal Machine Learning Algorithms for Cyber Threat Detection. In *2018 UKSim-AMSS 20th International Conference on Computer Modelling and Simulation (UKSim)*. Pp. 32–37. 2018.
doi:10.1109/UKSim.2018.00018

[NMYB17] R. Nokhbeh Zaeem, M. Manoharan, Y. Yang, K. S. Barber. Modeling and analysis of identity threat behaviors through text mining of identity theft stories. *Computers & Security* 65:50–63, 2017.
doi:https://doi.org/10.1016/j.cose.2016.11.002
https://www.sciencedirect.com/science/article/pii/S0167404816301559

[ZMB16] R. N. Zaeem, M. Manoharan, K. S. Barber. Risk Kit: Highlighting Vulnerable Identity Assets for Specific Age Groups. In *2016 European Intelligence and Security Informatics Conference (EISIC)*. Pp. 32–38. 2016.
doi:10.1109/EISIC.2016.014

[ZNB19] J. Zaiss, R. Nokhbeh Zaeem, K. S. Barber. Identity threat assessment and prediction. *Journal of Consumer Affairs* 53(1):58–70, 2019.