Automating Cyber-Attack Prediction using MITRE ATT&CK and Statistical Machine Learning Methods

Tobias Budig[a], Elisabeth Goebel[a], Tessa Fischer[a] and Jurek Muff[a]

[a]Karlsruhe Institute of Technology (KIT), Kaiserstraße 12, 76131 Karlsruhe, Germany

Abstract

Cyber-attacks have been a threat to companies, governments and society since the advancement of digitalisation. Since the covid-19 pandemic coveted and confidential patient data, information on vaccines and pandemic policies, as well as the increasing number of people working from home have exponentially increased the attack surface for attackers. To adequately counter this threat, new approaches are needed that enhance previous ideas. In recent years, a lot of research has been done to predict attacks on a technical and operational level. Here we propose a solution to identify trends in attack techniques based on past attacks. To do so, we propose to utilise clustering and time-series analysis as well as genetic algorithms. Furthermore, with this approach we try to identify new combinations of techniques that represent future threats. In this way, cyber-risk managers can perform intelligent and proactive investments, as well as staff training to give them advantage in the ongoing cat and mouse game. Moreover, this investigation helps to understand the evolution of cyber-attacks.

Keywords

cyber-attacks, strategic Cyber Threat Intelligence, Strategic Attack Predication

1. Introduction

Cyber-security has emerged as one of the most pressing issues confronting our globally connected world. Individuals, businesses and governments are becoming increasingly concerned about the costs and threats presented by cyber-crime, espionage, and cyber-warfare [1]. The mega-trend of digitalisation presents new challenges and potential for cyber-attacks.

The World Economic Forum estimated the damage related to worldwide cyber-crime to be $3 trillion in 2015. This number is expected to increase by 15% every year, reaching $10.5 trillion annually by 2025 [2] [3]. Protecting confidential data and defending private information against cyber-attacks has become an essential task for companies as well as governments. This threat is not limited to the IT sector but concerns any company dealing with confidential information like financial or medical data. The recent attacks on the Colonial Pipeline in the US showed how quickly cyber-attacks can happen and the significant impact they can have [4]. It revealed how vulnerable industries and governments are to even relatively basic assaults on their computer networks. This is unsurprising given how quickly the cyber-criminal world is evolving, such as through collaboration or automation and artificial intelligence to develop synergies for faster and more profitable exploitation of vulnerabilities. To counter this threat, new approaches and investments in the field of cyber-security are essential. It is expected that the worldwide information security market will reach $170.4 billion in 2022 [5].

This proposal will evaluate the hypothesis that data sets of historic malware and attack techniques can be used to predict future attack patterns. Recognising attack patterns and trends will help companies and institutions focus financial and human resources wisely to counter potential cyber-attacks. A deep understanding of attacker behaviour and the ability to predict trends counterbalances the disparity that attackers have through the first-mover advantage. Until now, the decision on which specific techniques to focus on has been based on expert experience rather than automated and traceable processes and metrics. This development of an automated prediction process is an essential step towards the strategic defence against such attacks. In the long run, this anticipation of attacks can be used to make companies aware of possible attacks even before they occur. Attackers have often already gained initial access and potentially compromised confidential data before the company reacts. As awareness is only the first step in protecting IT systems from future attacks, this automated prediction aims to prevent attacks in advance in the long run.

2. Problem

According to the Global Information Security Workforce Study, the global cyber-security workforce will be short by 1.8 million people by 2022, a 20% increase since 2015. 66% of respondents reported not having enough capacity to address current threats appropriately. The result-

tobias.budig@student.kit.edu (T. Budig);
elisabeth.goebel@student.kit.edu (E. Goebel);
tessa.fischer@student.kit.edu (T. Fischer);
jurek.muff@student.kit.edu (J. Muff)

ing consequences emphasize the importance of gaining knowledge about cyber-attacks to understand adversarial behaviour and increase the efficiency of dealing with threats. [6]

Understanding and analysing cyber-attacks that happened in the past and predicting patterns of attacks for the future means an improvement for cyber-security to enhance one's position in the ongoing cat and mouse game between adversaries and defenders. Therefore, predictive analysis would lead to an advantage for organisations to properly allocate their very scarce defence resources.

They could train their analysts to focus on the most significant parts of the cyber-defence based on historic data and not only on awareness through experience. Detection and response are the reality whereas prediction and prevention are the goals.

Automation processes such as auto-propagation systems have become more powerful in recent years [7]. Through these processes, attackers have an advantage as they are faster and can attack multiple weak points of companies at once. In fact, more than 90% of cyber-security specialists in the United States and Japan anticipate that attackers will utilize artificial intelligence against the companies they work for. While Automation and the use of, for example, artificial intelligence is commonly used by attackers, defenders on the other hand still have a lot of potential to improve their strategies and adapt them to new threats.[8]

Currently, companies are training with Red and Blue teams. In this process, the red team simulates attacks that the blue team tries to detect and responds accordingly. The better the Red team performs, the more possible vulnerabilities can be discovered. These simulations are with approximately $ 75,000 relatively expensive and only conditionally sustainable due to the growing number of threats. However, Red and Blue Teaming is among the most effective approaches to train the system and staff at the moment. [9]

Due to the lack of capacity and so far, few innovative approaches to counter attackers at the same level, it is necessary to find new solutions to allocate resources efficiently. Many studies have been conducted to predict techniques used during an attack at tactical and operational levels. This paper analyses strategic patterns and trends in the use of attack techniques. The aim is to give analysts an approach to better target investments, software, and staff training.

3. Past Work

So far, using predictive methods for strategic thread intelligence purposes has not been investigated in detail. Current solution options, methods and work are only applied in the operational and tactical domain, not at the strategic level. In the following section, we describe the current status based on the three pillars on which our work will be built:

1. The current state of research in strategic threat intelligence and cyber-situational awareness,
2. Predictive techniques with a focus on cyber security applications,
3. Terminology and framework by MITRE ATT&CK, a database framework of cyber-attacks.

3.1. Cyber situational awareness

To oversee the global evolution of cyber threats, one can use cyber situational awareness (CSA). This term leads to classical situational awareness. It is defined by Esley [10] as "Perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in near future." In cyber-security the situational awareness can be divided into three levels [11]. Monitoring cyber-systems and intrusion detection is part of the first level. Understanding the current cyber-security situation and its significance is represented by the second level, where modeling of threads or correlating security alters are used. The third level is called Projection and describes future states and events.

Cyber Situational Awareness is still a relevant topic in research. It deals with different cyber- security areas and a variety of issues related to this. While many research papers deal with CSA in a corporate context, some deal with cyber security issues concerning private users. The overarching goal for research questions in both sectors is, of course, to increase awareness among companies and individuals. One example for both sectors deals with personalized phishing mails, so-called spearphishing. Tools and visualization techniques have been developed to better assess the extent and impact of a cyber-attack. [12]. Research topics also include current trends such as the 5G infrastructure and IoT, the use of which is associated with security risks and awareness should therefore be created [13]. In the process, new approaches like anomaly ontology development and anomaly detection were developed to increase CSA.

3.2. Cyber threat intelligence

Cyber threat intelligence is often divided into three subcategories: operational, tactical and strategic threat intelligence.

Strategic threat intelligence provides a comprehensive picture of how the threat and attack landscape is evolving over time. Strategic intel can identify historical trends, motivations, or attributions as to who is behind

an attack. It is intended for high-level management to understand the current and future cyber threat situation. This strategic view enables management to implement defense mechanisms before the attacks even take place [14].

Strategic threat intelligence is at a high level where the exact technical aspects play a minor role compared to tactical and operational cyber threat intelligence. Nevertheless, especially for small and medium-sized businesses and companies, this strategic information is crucial since they often have limited financial and personnel resources.

3.3. Analytics and Prediction in Cyber-security

Researchers showed how discrete or continuous models and machine learning methods could be applied to the cyber-security sector in recent years. [Husák et. al] [15] wrote a detailed comparison of predictive methods in cyber-security and divided them into classes.

Attack projection assists the security analyst in identifying the next step of an adversarial. For instance, the Attack Hypothesis Generator by [Elitzur et al., 2019] performed significantly better than an analyst in estimating the next step of an ongoing cyber-attack[16]. They used a knowledge graph of historical malware based on the MITRE database. Then, they performed link predictions to predict the subsequent attack technique.

Intrusion prediction systems are monitoring organisation's networks. Another common technique is providing a honeypot as a trap for an adversary. Here, a server with known vulnerabilities is set up to attract an initial attack. Monitoring this server is now an early warning system. [Zhan et al., 2013] demonstrated an attack prediction up to five hours ahead based on the honeypot approach [17].

Network security situation forecasting supports the analyst to monitor the organisation's network traffic. It predicts future traffic based on historical observations to give alerts [18].

Each of the techniques mentioned above supports security analysts at an operational level in their day-to-day work. [Husa´k et al, 2018] showed that a wide range of prediction methods achieve up to 90% accuracy in recognising adversarial network behavior [15].

3.4. MITRE ATT&CK

MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) is a globally accessible curated knowledge base and a model about adversarial behaviour in cyber-attacks based on real-world observations. The MITRE Cooperation created ATT&CK out of the need to categorise and structure data of adversarial behaviour due to the increasing number and relevance of cyber-attacks.

Through ATT&CK, a common taxonomy has been created to help understand adversarial behaviour and improving defensive actions. ATT&CK is used as the foundation for developing specific threat models by researchers, analysts and developers. The first model was created in 2013, primarily focusing on the Windows enterprise environment. Since then, the database has been extended to other platforms such as Linux, macOS and Android.

The foundation of ATT&CK is based on various techniques an adversary can use, representing how an opponent will carry out an attack tactic. Each technique is associated with one or more tactics. Tactics can be understood as phases of an attack. These tactics answer the question why an adversary uses a particular technique. The sequence of several techniques used during an attack is defined as software. The software itself can be divided into malicious software (Malware) and legitimate software (Tools).

The most recent version of ATT&CK represents 552 techniques across 13 tactics and 585 different softwares. ATT&CK consists of two parts: The Enterprise version focuses on adversarial behaviour against enterprises, while the mobile version focuses on attacks against mobile devices.

4. Our Research Question

To support cyber-security staff on a strategic level we want to investigate two questions: Are there patterns or trends in the MITRE ATT&CK data set of malware? How do different algorithms perform to predict future malware? How different are the various metrics? To address these questions, we will describe our methodology as follows. First, we collected data about historic malware by scraping information about software and their used techniques from the MITRE ATT&CK website. Then, we cleaned the data and prepared them for further use.

As a next step, we propose first conducting a simple statistical analysis to identify the probability of techniques used by a software and the distribution of the number of techniques per software.

Building on these results, there is a possibility to provide insights into the most important techniques and how often they have been used in the past. Furthermore, this will provide decision-makers with data instead of intuition to guide their decision-making process. For the next step, a prediction of future combinations of techniques is desirable. Thereafter, we will compare approaches to predict impending attacks by fine-tuning the model by propagating trends.

Here we propose, on the one hand, to use a genetic algorithm to generate malware predictions. On the other hand, we want to make a dimensionality reduction, fol-

lowed by clustering approaches like k-means or hierarchical clustering of attack techniques inside an attack. A time-series or regression analysis will be conducted to identify trends inside these clusters. We want to split up the latest 20% of software from the data set to evaluate the proposed approaches. For time-series approaches, we will perform walk-forward validation. The nearest distance will evaluate the other approaches, like the genetic algorithm and the random baseline to one element of the test set.

In contrast to past work, we use predictive analytics not for operational but for strategic CTI. This will help cyber-security managers to make decisions based on data.

5. Conclusion & Impact

Predicting future cyber-attacks can help businesses, individuals and society. Understanding the past and predicting the future is an approach being sought in the course of time to develop new security profiles and software to help protect socially sensitive data and critical infrastructure from attackers. Knowledge and data mean power in these times, so protecting this data is one of our highest goals. In addition, cooperation between different associations is encouraged to share the findings and experiences and jointly find the best way to protect it and minimize the first-mover advantage of attackers.

References

[1] B. Oberzaucher, 2019. URL: https://www.andritz.com/spectrum-en/latest-issues/issue-39/digitalization-as-a-megatrend.

[2] The emerging era of cyber defense and cybercrime, 2016. URL: https://www.microsoft.com/security/blog/2016/01/27/the-emerging-era-of-cyber-defense-and-cybercrime/.

[3] D. Freeze, Cybercrime to cost the world $10.5 trillion annually by 2025, 2021. URL: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.

[4] P. Sanger, Pipeline attack yields urgent lessons about u.s. cybersecurity, 2021. URL: https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html.

[5] R. Contu, Forecast analysis: Information security, worldwide, 2q18 update, 2018. URL: https://www.gartner.com/en/documents/3889055.

[6] Frost and Sullivan, 2017 global information security workforce study, 2017.

[7] B. Buchanan, J. Bansemer, D. Cary, J. Lucas, M. Musser, Automating cyber attacks (2020).

[8] R. Goosen, A. Rontojannis, S. Deutscher, J. Rogg, W. Bohmayr, D. Mkrtchian, Artificial intelligence is a threat to cybersecurity. it's also a solution., 2021. URL: https://www.bcg.com/publications/2018/artificial-intelligence-threat-cybersecurity-solution.

[9] L. Antoniou, Marketplace, red team / blue team exercise, 2021. URL: https://aws.amazon.com/marketplace/pp/prodview-yj24julw7uvsc.

[10] M. R. Endsley, Situation awareness global assessment technique (sagat), in: Proceedings of the IEEE 1988 national aerospace and electronics conference, IEEE, 1988, pp. 789–795.

[11] M. R. Endsley, Toward a theory of situation awareness in dynamic systems, in: Situational awareness, Routledge, 2017, pp. 9–42.

[12] P. Legg, T. Blackman, Tools and techniques for improving cyber situational awareness of targeted phishing attacks, in: 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), IEEE, 2019, pp. 1–4.

[13] E. Chang, F. Gottwalt, Y. Zhang, Cyber situational awareness for cps, 5g and iot, in: Frontiers in Electronic Technologies, Springer, 2017, pp. 147–161.

[14] W. Tounsi, H. Rais, A survey on technical threat intelligence in the age of sophisticated cyber attacks, Computers & security 72 (2018) 212–233.

[15] M. Husák, J. Komárková, E. Bou-Harb, P. Čeleda, Survey of attack projection, prediction, and forecasting in cyber security, IEEE Communications Surveys & Tutorials 21 (2018) 640–660.

[16] A. Elitzur, R. Puzis, P. Zilberman, Attack hypothesis generation, in: 2019 European Intelligence and Security Informatics Conference (EISIC), IEEE, 2019, pp. 40–47.

[17] Z. Zhan, M. Xu, S. Xu, Characterizing honeypot-captured cyber attacks: Statistical framework and case study, IEEE Transactions on Information Forensics and Security 8 (2013) 1775–1789.

[18] L. Shang, W. Zhao, J. Zhang, Q. Fu, Q. Zhao, Y. Yang, Network security situation prediction based on long short-term memory network, in: 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS), IEEE, 2019, pp. 1–4.