Attack Forecast and Prediction

Florian Klaus Kaiser[a], Tobias Budig[a], Elisabeth Goebel[a], Tessa Fischer[a], Jurek Muff[a], Marcus Wiens[a] and Frank Schultmann[a,b]

[a] Karlsruhe Institute of Technology (KIT), Kaiserstraße 12, 76131 Karlsruhe, Germany
[b] Adelaide Business School, University of Adelaide, 12/10 Pulteney Street, Adelaide, Australia

Abstract

Cyber-security has emerged as one of the most pressing issues for society with actors trying to use offensive capabilities and those who try to leverage on defensive capabilities to secure their assets or knowledge. However, in cyber-space attackers oftentimes have a significant first mover advantage leading to a dynamic cat and mouse game with defenders. Cyber Treat Intelligence (CTI) on past attacks bears potentials that can be used by means of predictive analytics to minimise the attackers first mover advantage. Yet, attack prediction is not an established means and automation levels are low.

Within this work, we present Attack Forecast and Prediction (*AFP*) which is based on MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK). *AFP* consists of four modules representing different analytical procedures which are clustering, link prediction, time series analysis, and genetic algorithms. *AFP* identifies trends in the usage of attack techniques and crafts forecasts and predictions on future malware and the attack techniques used. We rely on time sorting to generate subgraphs of MITRE ATT&CK and evaluate the accuracy of predictions generated by *AFP* based on these.

Keywords

Attack Prediction, Cyber Threat Intelligence, Genetic Algorithms

1. Introduction

1.1. Motivation

Cyber-security has emerged as one of the most pressing issues confronting our globally connected world. 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 [1] [2]. Consequently, individuals, businesses and governments are becoming increasingly concerned about the costs and threats presented by cyber-crime, espionage, and cyber-warfare [3]. It is expected that the worldwide information security market will reach $170.4 billion in 2022 [4].

Attackers' strategies quickly develop and are subject to dynamic innovations. This is, the cyber-criminal world is evolving to exploit vulnerabilities in a faster and more profitable way. To counter this threat, new approaches and investments in the field of cyber-security are essential. "The capabilities, persistence, and complexity of adversarial attacks in the present threat landscape result in a speed race between security analysts, incident responders, and threat actors."[5] Thereby the attacker seems to have a *first mover advantage* Thus companies are often vulnerable even to relatively basic assaults on their computer networks.

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 [6]. 66% of respondents reported not having enough capacity to address current threats appropriately. The resulting consequences emphasise 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 of cyber-security in its ability to enhance one's position in the arms race between adversaries and defenders.

Therefore, predictive analysis could lead to an advantage for organisations to properly allocate their scarce defence resources. Although predicting attacks is not a new procedure, automating attack forecasting and predictions were options hardly used in the past. Rather, attack predictions were largely based on subjective perceptions of experienced experts from the cyber-threat landscape. Yet, experienced experts are rare and their time is even scarcer.

Automation of attack forecasting and predictions would substantially decrease biases in predictions and minimise experts' time spending on generating forecasts.

1.2. Problem statement

Predicting future malware and their functioning is hence of especial interest. Furthermore, predictions can increase cyber-security maturity. Research and develop-

florian-klaus.kaiser@kit.edu (F. K. Kaiser); 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); marcus.wiens@kit.edu (M. Wiens); frank.schultmann@kit.edu (F. Schultmann)

CEUR Workshop Proceedings (CEUR-WS.org)

ment of defensive measures take a lot of time, whereas better prediction can reduce the time lead over attackers. Note that security spending is an investment in the future security of a company and should hence follow the dynamics of attacks. CTI (e.g. as it is provided by MITRE ATT&CK; for an in depth discussion on CTI and the relation to MITRE ATT&CK refer to section 2) represents an opportunity for making predictions more accurate. However, currently, predictions on future developments of attacks are rare and oftentimes are largely based on experiences of some analysts rather than CTI. This low level of automation regarding the prediction causes many problems for cyber-security. First, experts were distracted from their operations and generating predictions means extra workload for them. Second, even the best and experienced experts perceive cyber-attacks only from a limited and in this way subjective, perspective. This is, human crafted predictions are prone to biases.

1.3. Research question and course of the study

To support cyber-security staff on a strategic level and make predictions on the development of attacks more accurate, we investigate two questions:

i Are there any patterns or trends in the MITRE ATT&CK that can be used for crafting medium to long term predictions on the threat landscape?
ii How do different algorithms perform to predict future malware?

To address these questions, we collect data about historic malware by scraping information about software and their used techniques from the MITRE ATT&CK database. Then, we clean the data and prepare them for further use. In a next step, we first conduct 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 compare approaches to predict impending attacks by fine-tuning the model by propagating trends.

Here we propose, on the one hand, to use genetic algorithms to generate malware predictions [7]. On the other hand, we make a dimensional reduction, followed by clustering approaches like k-means or hierarchical clustering. A time-series and regression analysis is be conducted to identify trends inside these clusters [8] [9].

To evaluate our algorithms we craft subgraphs from knowledge graphs using time sorting and run the analysis on real data (knowledge at a specific point in time). 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 (please refer to section 2), we use predictive analytics not on an operational but on a strategic level.

1.4. Contribution

In this work, we present *AFP* taking advantage of CTI for automatically crafting predictions on future malware and their attack techniques used. In doing so, *AFP* leverages on CTI to infer patterns within time series of attacks, making it possible to gain insights to attack evolution and development as well as deriving further relevant information (e.g. the popularity of specific attack techniques) and crafts forecasts based on this information. In this way, analysts, researchers and security managers can gain insights into the future cyber-threat landscape and prepare proactively for threats that are likely to occur in the future. Additionally, cyber-risk managers can perform intelligent and proactive investments relying on *AFP*, as well as staff training to minimise the attackers' first mover advantage. The ability of *AFP* to predict the future course and the development of the threat landscape is a critical step towards increasing levels of cyber-defence and security as well as its automation. The development of an automated prediction process is an essential step towards the strategic defence against cyber-attacks and can significantly increase cyber security maturity for non-specific attacks. In the long run, this anticipation of attacks can be expanded and used for successful attack prevention.

2. State of research and related work

2.1. Cyber-situational awareness

Situational awareness describes the "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."[10] In the context of cyber-security, situational awareness can be divided into three levels [11]. These are (1) monitoring of cyber-systems and intrusion detection, (2) understanding of the current situation and its significance for cyber-security, and (3) projection. The last aspect includes predictive capabilities and is hence the joint link to this work.

2.2. Cyber threat intelligence

CTI is structured information extracted from monitored systems or intrusion detection systems [12]. It includes actionable information on past attacks (evidence based knowledge). CTI is often divided into four subcategories: (1) technical (2) operational, (3) tactical, and (4) strategic threat intelligence [13]. It includes tactics, techniques and attack patterns (TTPs), indicators of compromise (IOCs), tools, threat actors, date of discovery, and other information. Information extracted from various sources of CTI is leveraged by many analysts to increase the efficiency of defensive measures such as anomaly detection systems, intrusion detection systems, and threat hunting [12].

Since a single individual, security analyst, security researcher or any other expert cannot acquire all information on all threats, there is a high importance of sharing CTI among different stakeholders to enable a holistic perspective [12]. Hence, there were great efforts to formalise and standardise threat sharing and to develop a common language. One of those languages is the Structured Threat Information eXpression (STIX) language [1], which is also utilised by MITRE ATT&CK[2].

MITRE 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 MITRE ATT&CK, a common taxonomy has been created to help understand adversarial behaviour and improving defensive actions. MITRE 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 MITRE 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 and are therefore consistent to the cyber kill chain [14]. 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 MITRE ATT&CK represents 552 techniques across 13 tactics and 585 different softwares. MITRE 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.

Furthermore, beside CTI for attacker modelling, there is also information on defender modelling including information on system vulnerabilities. This is for example the National Vulnerability Database (NVD)[3] or the Common Vulnerabilities and Exposures (CVE) database[4]. This information can be used to understand trends, patterns and developments in software vulnerabilities that would affect the threat landscape.

2.3. CTI based predictions for 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 [9] made a detailed comparison of predictive methods applicable for both long term investigations and forecasts as well as short term predictions, e.g. used for efficient threat hunting in cyber-security and divided them into classes.

2.3.1. Short term predictions

Short-term attack projection assists security analysts in identifying the next step of an adversary. One example is the Attack Hypothesis Generator (AHG) by Elitzur et al. [12]. Within their work, they used a knowledge graph of historical malware based on the MITRE ATT&CK, AlienVault Open Threat Exchange (OTX), and VirusTotal. Based on the knowledge graph, they predict subsequent and linked attack techniques given some currently observed data. AHG performed significantly better than an analyst in estimating the next step of an ongoing cyber-attack [12]. Within their work, Elitzur et al. [12] proved that short term predictions can be beneficial for improving cyber-security and setting efficient defensive measures at place.

Furthermore, Zhan et al. [15] demonstrated the usage of short term attack predictions relying on honeypots. They enabled attack predictions up to five hours ahead based on data gained from their honeypot. Furthermore, Fava et al. [16] presents a methodology for projecting attacks based on information gathered from Intrusion Detection Systems (IDS).

Each of the techniques mentioned above craft predictions to support security analysts at an operational level in their day-to-day work. Husák et al. [9] showed that

[1] https://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/stix-20-finish-line

[2] https://attack.mitre.org/

[3] https://nvd.nist.gov/

[4] https://cve.mitre.org/

a wide range of prediction methods achieve up to 90% accuracy in recognising adversarial network behaviour.

Further works are inter alia given by Qin and Lee [17]

2.3.2. Medium to long term predictions

Zhang et al. [18] provide a study applying data-mining and machine learning for predicting the "time to next vulnerability for a given software application". However, they concluded that the NVD has only low predictive power. This might be as there is a close link between the occurrence of new attacks and the exploitation of vulnerabilities. Furthermore, Ozment [19] highlighted that there is not enough information in freely accessible vulnerability databases including NVD. This is, CTI about attacks might have a higher predictive power than data on vulnerabilities. Further contributions investigating the possibility of predicting vulnerabilities include the works from Alhazmi and Malaiya [20], Abraham and Nahir [21] ,and Nguyen and Tran [22].

3. Conclusion & impact

Improving defensive capabilities in cyberspace for improving cyber-security is one of the key challenges that need to be solved to enable resilient societies and modern life, which is increasingly penetrated by information technology.

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. Predicting future cyber-attacks can help businesses, individuals and society. Minimising attackers first mover advantage therefore need to be a focal point of research. Yet, it is barely considered or largely based on subjective opinions and biased by individual perspectives of experts. With our work we aim at overcoming these shortcomings and forward research in the field of attack forecasting and prediction.

References

[1] P. Boden, 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/.

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

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

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

[5] V. Mavroeidis, S. Bromander, Cyber threat intelligence model: an evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence, in: 2017 European Intelligence and Security Informatics Conference (EISIC), IEEE, 2017, pp. 91–98.

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

[7] S. Ijaz, F. A. Hashmi, S. Asghar, M. Alam, Vector based genetic algorithm to optimize predictive analysis in network security, Applied Intelligence 48 (2018) 1086–1096.

[8] S. J. Yang, H. Du, J. Holsopple, M. Sudit, Attack projection, Cyber Defense and Situational Awareness (2014) 239–261.

[9] 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.

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

[13] D. Chismon, M. Ruks, Threat intelligence: Collecting, analysing, evaluating, Technical Report, MWR InfoSecurity, 2015.

[14] E. M. Hutchins, M. J. Cloppert, R. M. Amin, Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains, Leading Issues in Information Warfare & Security Research 1 (2011) 80.

[15] 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.

[16] D. S. Fava, S. R. Byers, S. J. Yang, Projecting cyberattacks through variable-length markov models, IEEE Transactions on Information Forensics and Security 3 (2008) 359–369.

[17] X. Qin, W. Lee, Attack plan recognition and prediction using causal networks, in: 20th Annual Computer Security Applications Conference, IEEE, 2004, pp. 370–379.

[18] S. Zhang, X. Ou, D. Caragea, Predicting cyber risks through national vulnerability database, In-

formation Security Journal: A Global Perspective 24 (2015) 194–206.
[19] J. A. Ozment, Vulnerability discovery & software security, Ph.D. thesis, University of Cambridge, 2007.
[20] O. H. Alhazmi, Y. K. Malaiya, Prediction capabilities of vulnerability discovery models, in: RAMS'06. Annual Reliability and Maintainability Symposium, 2006., IEEE, 2006, pp. 86–91.
[21] S. Abraham, S. Nair, A predictive framework for cyber security analytics using attack graphs, arXiv preprint arXiv:1502.01240 (2015).
[22] V. H. Nguyen, L. M. S. Tran, Predicting vulnerable software components with dependency graphs, in: Proceedings of the 6th International Workshop on Security Measurements and Metrics, 2010, pp. 1–8.