Brief Report

Multi-Stage Attacks: Concepts, Detection and Defences

Wahab Khan *

Posted Date: 15 June 2023

doi: 10.20944/preprints202306.1085.v1

Keywords: Multi-stage attack; detection; Advanced Persistent Threats; cyberattack; defence mech- anisms

Brief Report

Multi-Stage Attacks: Concepts, Detection and Defences

Wahab Ali Khan

University of Bradford, Bradford, United Kingdom; wakhan3@bradford.ac.uk

Abstract: The need for cohesive detection and defence methods against cyberattacks is significant now more than ever before to enforce security and privacy of user data and information. The inevitable increase in demand for home and flexible working from employees quite recently has meant there is a lack of awareness and training for cyberattacks. Hence, they have become prominent as attackers are aware of this and are benefitting from individuals' lack of knowledge in how to better protect themselves and their confidential information. Employees are becoming more susceptible to such attacks and falling victim to these, resulting in economic losses for companies, data losses and decreased faith.

Keywords: multi-stage attack; detection; Advanced Persistent Threats; cyberattack; defence mechanisms

I. Introduction

The current evolution of technology can prove to be quite confusing to individuals in terms of navigation which can lead to them being more vulnerable to cyberattacks. The increased complexity can mean individuals are not aware of how to better protect themselves against such attacks and in general their data and information. This can mean they are more at risk of being tricked through content appearing to be legitimate but in fact having malicious effects, one such instance is social engineering where the user is manipulated into providing their sensitive and confidential information that will be of benefit to attackers.

Attacks target weaknesses, exploiting visible vulnerabilities to affect users. They focus on extracting victim information and data for a variety of purposes such as committing fraud. In the case of employees, they are used as means for attackers to attain vital company data that can be sold or modified. This can lead to negative effects on company image and reputation. One of the more complex and severe cyberattacks is the multi-stage attack, commonly referred to as a multi-step attack, with different variations e.g., Advanced Persistent Threats (APTs) making it more of a concern to organisations, individuals, and governments due to the threat(s) that these attacks carry [1]. As it exists today, some detection approaches address a minority of the challenges these attacks highlight. However, technological limitations and cyberattack advancements mean that all fail to shutdown these attacks. Understanding the areas of concern is key in the investigation of why current methods neglect the major issues and showcases how they can be further improved to ensure the prevention of such attacks.

Multi-stage attacks explicitly defined in their name work by executing several stages to attack users. As of now, it is known that multi-stage attacks utilise methods such as phishing scams in the form of emails most commonly to deceive recipients into clicking on malicious links. Which is where a dropper file is delivered; clicking on the link leads to the opening of this and a hidden payload being executed. This contains the malicious content of the multi-stage attack in the form of code that is executed on the user system.

Warranting the defence of personal devices is important as multi-stage attacks can take advantage of any weakness or vulnerability that users pose. Early detection of these attacks can also prove to be useful and implementation of defence methods in companies to mitigate the risk of these attacks on their systems and networks.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 June 2023 doi:10.20944/preprints202306.1085.v1

The lack of knowledge in multi-stage attacks is evident in the defence mechanisms that exist today due to their insufficiency of tackling the security challenges that individuals and organisations face. The reason for this is that the multi-stage attack process requires a full understanding to detect the threat. However, such detection methods e.g., intrusion detection lacks this and thus consequent in a delay of identifying the issue [2]. Moreover, organisations have predominantly become susceptible to multi-stage attacks due to the increase in risks that has resulted from the exponential expansion of systems and devices connected to networks and the internet. Such attacks involve many phases that are rationally performed for effective outcomes [3].

Many research papers and studies scope the advancements of multi-stage attacks but, new developments in defence investigations have proven to overcome many of the attack's concerns in which this paper will explore by contributing to the analysis of multi-stage attacks with a deeper understanding of the concepts, detection methods and defence mechanisms [16–18].

The paper structure is as follows: Section 2 discusses the concepts of multi-stage attacks including the lifecycle and examples of the attack; Section 3 will follow up with detection and defence methods; Section 4 will cover a discussion and critical analysis and finally, conclusion statements will be included in the last section of the paper.

II. Concepts

A multi-stage attack can be defined as a complex intrusion method that can be used to infiltrate network infrastructures through various stages and can bypass detection methods as they cannot handle the many stages that are included in the long sequence of the attack [4]. Due to the complexity and bypassing techniques the attack implements and in the attacker's strategy, it becomes one of the more severe cyberattacks and will require strong and reliable defences to ensure safety becomes the priority in the face of the attack.

Multi-stage attacks can be defined as 2 types, one of the types compromises as many systems as it can in a connected network e.g., [5, Figure 1] the WannaCry. The other type of multistage attack is defined as taking many steps to compromise its target within the network e.g., DARPA 2000 dataset. Figure 1 [5] presents a multi-stage attack example where the first step is for the attacker to compromise the user or desktop through a gateway or web server by exploiting some of the vulnerabilities that exist in those access points. Once exploited, the attacker can access the local desktop [5].

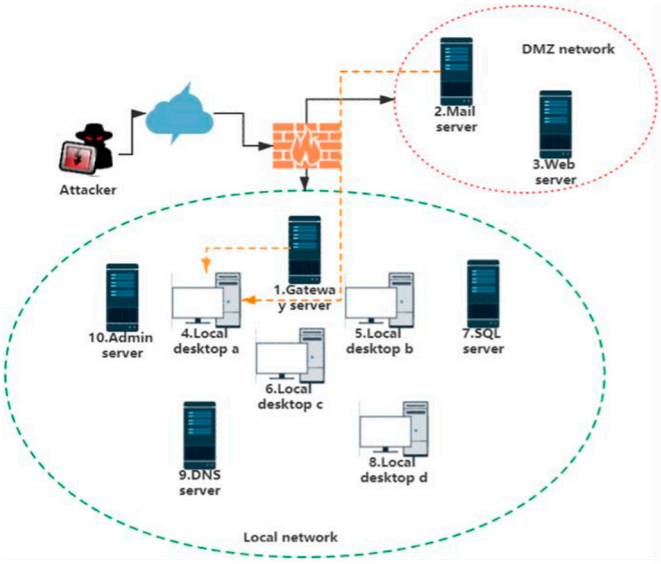

Figure 1. An example of a multi-stage attack.

Some examples of real-life multi-stage attacks exist such as the WannaCry attack that affected critical infrastructure devices of hospitals and public transport systems causing many system

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 June 2023 doi:10.20944/preprints202306.1085.v1

malfunctions as these devices were associated with intermediate networks and the Internet [6]. Other multi-stage attacks exist such as the Advanced Persistent Threats (APTs) which are persistent, multi-stage attacks that can cause such damage on a global and financial scale through collecting information from marked systems that are targeted through exploits [7].

Multi-stage attacks have evolved overtime due to the nature of detection and prevention techniques leading to security measures and decrease in vulnerability exposure for attackers. However, these said attacks have matured in ways that current prevention methods may not be able to tackle as the complexity they possess. For example, the attack was first structured as a single multi-stage attack but as defence mechanisms evolved, multi-stage attacks adapted to avoid any conflicts with prevention methods by evolving their attack strategy and interweaving with other attacks [19]. This has proven to harden the attack implementation and increase the severity in damages that the attack causes.

III. Detection and Defence Methods

As per any cyberattack, multi-stage attacks are no different when discussing detection and prevention methods to hinder and stop the incidents from occurring. Early detection methods to identify some obsolete multi-stage attacks include but are not limited to Causal-Correlation or Causal-based. However, due to the general expansion of the attack and minimal access to the required datasets these methods cannot overcome today's advancements in such attacks [8]. Nowadays, several defence approaches for multi-stage attacks are unable to track the whole cycle of the attack but rather only detect single stage or each phase of an attack posing a threat to all detection methods, current and new [20]. This is furthered by various multistage attacks that are intertwined. Therefore, cyber systems must ensure that they are developed with a prioritised necessity that is a complex detection and prediction multistage attack approach [9]. Due to the complexity of multi-stage attacks, detecting the attack is only feasible through merging different subsystems' data to ensure an effective detection strategy as a lone subsystem is deficient in overcoming the attack [10]. However, it has been stated that multi-stage attacks typically leave traces when intruding networks and can be detected and collected using a security system such as a System of Information and Event Management (SIEM). This system can detect the threats of the attack and can notify users through a system interface [11].

Some multi-stage attacks such as Advanced Persistent Threats (APTs) attacks require full detection methods as early detection technologies do not suffice. This is due to how APTs use a slow-and-low attack strategy which helps to increase the period and stages in which the attack is active [12]. Other detection methods e.g., firewalls could help in slowing down the attack but does not have the capacity to prevent the attack due to the complexity of APTs. Firewalls can prevent possible threats through eliminating unauthorised packets in accordance with the policy applied. This type of mechanism is seen as a simple and common defence that is flexible in its ability to deploy and adjust its compliance; however such freedom can result in harmful actions through low-security firewalls whereas high security firewalls ensure low to no threats [13].

Predicting multi-stage attacks has become increasingly difficult due to the lack of current approaches that exist. However, through investigation of recent advancements Hidden Markov Models (HMM) is seen to be a prominent approach in the prediction of multi-stage attacks as the models can track multi-stage through their ability to handle sequential data. Although this may be the case, there remains the challenge that is interleaving multi-stage attacks and evaluating the performance of detection methods which includes HMM failing to address this as their focus remains on single multistage attacks [14]. An evaluation of multi-step attacks and their prediction mechanisms was conducted through a survey in which the outcomes outlined how problematic it was to identify the attacks [21,22]. The results included difficulty in comparing the attacks through detection as the approach to determine the attacker's strategy was insufficient. Another issue was the limited access of network data and the complexity to access this including the challenge of retrieving filtered network information [15].

 doi:10.20944/preprints202306.1085.v1

IV. Discussion

Thorough research and investigation of review papers into multi-stage attacks and the detection, defence and prevention schemes in place have all outlined the dangers of multistage attacks and have all proposed solutions or further and future work that can be conducted to help hinder and prevent damage that can be caused. However, much like all proposed solutions the above also lack some of the techniques that are required to detect and stop the attacks due to the complexity and architecture of the attack and its ability to take shape in different types as well as evolve through technological advancements further than the security progression.

The consequences of multi-stage attacks can bleed into individual and organisational structures if not properly attended to. An example of this resides in an employee receiving a phishing email or message that contains false or leading information and a link that may redirect the employee to a malicious site or domain. The employee may have received this as their email or some credentials may have been leaked, passed through, or used as a registration with or without consent or full authorisation. Once entered, the attacker can then discover any vulnerabilities in the architecture of the systems and networks and exploit them to create back doors or access points to control or for later use. The exploits are utilised by deploying the attack through the attacker's strategy of multiple phases to bypass and hinder detection methods. In doing so, the attacker can collect data and cause severe damage on a financial and organisational scale where profits and personal credentials of other employees can be leaked. This could be furthered by a damaged reputation that could lead to a loss in their customer base and could be potentially costly due to the time it would take to recover from all losses.

The studies and proposed solutions offer use cases and scenarios in which their ideas would be most applicable however, as all proposals these are happy paths and do not present edge or extreme cases in which attackers would seek out to exploit in these methods. Prevention techniques would be more important than ever in the scenario of an organisation attack using multi-stage attack strategies. Ensuring that all employees are well equipped with sufficient knowledge and are made vigilant and aware of such cases could help in reducing the effects of attacks and can overall contribute to the security of the organisation and individuals.

The SIEM approach as proposed by Navarro [11] would help in detecting the attack at its early stages where the severity of the damage would be less, helping to overcome the attack and enforce protocols and procedures to ensure high security measures. This method however would only notify of the attack and would be up to the victims to act which in the grand scheme of things could be time costly. Due to this factor, this detection method although reliable in some respects cannot be utilised as the single security approach to safeguard individuals and organisations alike.

Other defence approaches include Hidden Markov Models (HMM) and their ability to track the attack through handling sequential data. Although the approach may be able to penetrate the multi-stage attack in this form, there leaves the issue of interleaving multi-stage attacks which this method is unable to apprehend like many other defences discussed. Other detection methods may be seen as unreliable as their capacity is only able to detect single stage attacks also.

One of the biggest issues that still haunts victims and organisations in general is the ability of attackers to adapt their attacking techniques once a prevention method prevails in eliminating one of the threats that multi-stage attacks possess. Due to the collection of data and power that attackers can gain control of using such attacks, they will continue to implement and victimise many in their attempt to gain that data and power to use to their aid. Such that it is best to ensure that research is thoroughly conducted and continued to investigate further how multi-stage attacks can evolve so evasive actions can be taken to ensure security and prevention software lead the race in stopping multi-stage attacks from taking place.

Considering all discussion points, multi-stage attacks will only evolve into much greater threats that will require further research and commitment to ensure they are dealt with, and that the severity of the attacks do not impact individuals' and organisations' security and privacy.

V. Conclusions

To conclude this review of multi-stage attacks, the threat still looms over at a global scale, more predominantly on individuals and organisations as they can be viewed as easy targets through exploiting vulnerabilities that are not made aware of. There are cases where multi-stage attack preventions have been successful but with the rise in technological advancements and increase in security flaws, the attack strategy has also progressed to evade most, if not all, prevention attempts, worsening the overall attempt to tackle challenge.

The detection and defence mechanisms in place have generally been successful in preventing multi-stage attacks but are still far from completion as they lack advancements to address many of the attack principles the multi-stage attack adheres to. Looking at the effects of multi-stage attacks further in respects to individual and organisational severity effects can help in understanding the techniques that can be undertaken to lessen the attack damages. Ensuring that individuals and organisations are made aware of attack strategies and are knowledgeable on the protocols that should take place should such a case arise is one of the steps forward in decreasing the attacks percentage. Also, taking precaution when visiting sites or reviewing attachments and links can be furthered to ensure that no vulnerabilities are exploited. As for exploits, using stateof-the-art and reliable vulnerability software could aid in patching and remove any exploits that attackers could take advantage of.

The above however may not still eliminate multi-stage attack attempts as attackers will always trial and error techniques to evade all prevention methods and will continue to advance their technology and strategies to ensure the security measures in place fall behind. This does suggest there is room for improvement in all areas and aspects of multi-stage attack prevention and is up to individuals and organisations to consistently practise security protocols to not fall victim to attackers.

An attempt at further and future work could be to research current approaches and how they can be improved to identify all multi-stage attack issues at all levels. This could be either through investigation or evaluation of how each method works against a dummy multi-stage attack. Understanding where the key pitfalls are of each method could be the pivotal direction in which these methods could turn around to successfully eliminate multi-stage attack threats. Other further work that could be seen as less time costly could be on how the existing defence mechanisms can be interwoven to work simultaneously and as one force to overcome multi-stage attacks in their various forms and attack tactics. This would require the work of many proposed approaches to formulate an understanding on how all would complement each other and work in harmony. Although this may be the desired approach, the resources and capacity available may hinder the progress of this method or in fact all techniques contribute to the fall of multi-stage attacks.

References

[1] Y. Takey, S. Tatikayala, S. Samavedam, P. Eswari and M. Patil, “Real Time early Multi Stage Attack Detection,” presented at the 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2021, pp. 283-290.

[2] I. Ghafir and V. Prenosil, “Advanced Persistent Threat and Spear Phishing Emails.” International Conference Distance Learning, Simulation and Communication. Brno, Czech Republic, pp. 34-41, 2015.

[3] J. Navarro, A. Deruyver and P. Parrend, “A systematic survey on multistep attack detection,”Journal of Computers and Security vol. 76, pp. [35 pages], Mar. 2018.

[4] T. Mezeˊ sovˇ a, P. Sokol, and T. Bajtoˊ s, “Evaluation of Attackers’ Skillˇ Levels in Multi-Stage Attacks,” Journal in Information, vol. 11, no. 11, pp. [15 pages], Nov. 2020.

[5] P. Zhou, G. Zhou, D. Wu and M. Fei, “Detecting multi-stage attacks using sequence-to-sequence model,” Journal in Computers Security, vol. 105, pp. [15 pages], Feb. 2021.

[6] Z. Hu, M. Zhu and P. Liu, “Adaptive Cyber Defense Against Multi-Stage Attacks Using Learning-Based POMDP,” Journal of ACM Transactions on Privacy and Security, vol. 24, no. 1, pp. [25 pages], Feb. 2021.

[7] M. Hammoudeh, I. Ghafir, A.Bounceur and T. Rawlinson, “Continuous Monitoring in Mission-Critical Applications Using the Internet of Things and Blockchain,” International Conference on Future Networks and Distributed Systems. Paris, France, 2019.

[8] I. Ghafir and V. Prenosil, “Blacklist-based Malicious IP Traffic Detection,” Global Conference on Communication Technologies (GCCT). Thuckalay, India: pp. 229-233, 2015.

[9] A. Zimba, Z. Wang, H. Chen, “Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems,” Journal in ICT Express, vol. 4, no. 1, pp. [4 pages], Jan. 2018.

[10] I. Ghafir et al., “Detection of advanced persistent threat using machine learning correlation analysis,” Journal in Future Generation Computer Systems, vol. 89, pp. 349-359, Dec. 2018.

[11] B. Jia, Y. Tian, Di, Zhao, X. Wang, C. Li, W, Niu, E. Tong and J, Liu, “Bidirectional RNN-Based Few-Shot Training for Detecting Multi-stage Attack,” in Information Security and Cryptology, Y. Wu and M. Yung, Eds. Guangzhou, China: Springer International Publishing, 2021, ch. 1, pp. 3752.

[12] S. Eltanani and I. Ghafir, "Aerial Wireless Networks: Proposed Solution for Coverage Optimisation," IEEE Conference on Computer Communications Workshops”, IEEE, 2021.

[13] I. Ghafir and V. Prenosil. “Proposed Approach for Targeted Attacks Detection,” Advanced Computer and Communication Engineering Technology, Lecture Notes in Electrical Engineering. Phuket: Springer International Publishing, vol. 362, pp. 73-80, 9, 2016.

[14] T. Shawly, M. Khayat, A. Elghariani and A. Ghafoor, “Evaluation of HMMBased Network Intrusion Detection System for Multiple MultiStage Attacks,”Journal in IEEE Network, vol. 34, no. 3, pp. [8 pages], Mar. 2020.

[15] X. Li, M. Xu, P. Vijayakumar, N. Kumar and X. Liu, “Detection of LowFrequency and Multi-Stage Attacks in Industrial Internet of Things,” Journal in IEEE Transactions on Vehicular Technology, vol. 69, no. 8, pp. [11 pages], May. 2020.

[16] J. Navarro, V. Legrand, A. Deruyver and P. Parrend, “OMMA: open architecture for Operator-guided Monitoring of Multi-step Attacks,” EURASIP Journal in Information Security, vol. 6, pp. [25 pages], May. 2018.

[17] I. Ghafir and V. Prenosil, “Malicious File Hash Detection and Drive-by Download Attacks,” International Conference on Computer and Communication Technologies, series Advances in Intelligent Systems and Computing. Hyderabad: Springer, vol. 379, pp. 661-669, 2016.

[18] A. Zimba, H. Chen, Z. Wang and M. Chishimba, “Modelling and detection of the multi-stages of Advanced Persistent Threats attacks based on semi-supervised learning and complex networks characteristics,” Journal in Future Generation Computer Systems, vol. 106, pp. [16 pages], May. 2020.

[19] J. Shin, S. Choi, P. Liu and Y. Choi, “Unsupervised multi-stage attack detection framework without details on single-stage attacks,” Journal in Future Generation Computer Systems, vol. 100, pp. [14 pages], May. 2019.

[20] I. Ghafir, J. Svoboda, V. Prenosil, “A Survey on Botnet Command and Control Traffic Detection,” International Journal of Advances in Computer Networks and Its Security (IJCNS), vol. 5(2), pp. 75-80, 2015.

[21] T. Shawly, A. Elghariani, J. Kobes and A. Ghafoor, “Architectures for Detecting Interleaved Multi-Stage Network Attacks Using Hidden Markov Models,” Journal in IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 5, pp. [14 pages], Oct. 2019.

[22] N. Helmut, M. Winter, B. Stojanovic, K. Hofer-Schmitz, J. Bo´ zi˘ c and´ U. Kleb, “APT-Attack Detection Based on Multi-Stage Autoencoders,” Journal of Applied Sciences, vol. 12, no.13, pp. [18 pages], July. 2022.