Multi-stage attack: concepts, detection and defence

By Ariane Garrett

***Abstract* — In recent years, cyber security has experienced several challenges due to the exponential growth of the internet and the impact of it worldwide. Nowadays, it is nearly impossible to live without being connected, and, even if this has its positive side, there are also many dangers that come along the use of the internet. Day after day we find about new cyber-attacks all around the world, some of these being harder to understand than others, becoming incredibly hard to control or even to prevent them. The following report will focus on one of the toughest types of attacks that exists, the multi-stage attack, which pretends to perpetrate a cyber-attack that affects the target in more than one stage. It will also be discussed the different detection approaches and types that exist, and how helpful these are to identify if the attack is a multi-stage one or not, so this way we can be sure about what we are facing. Finally, different prevention mechanisms will be discussed, and how these are helpful against multi-stage attacks.**

Keywords* — *multi-stage attacks, cyber-attacks, stage, target, victim, attacker, network, system, machine, detection, method, attack path, malicious, threat, prevention.

I. Introduction

During the modern era, internet has become an essential part of our lives, and as funny, entertaining and captivating it can be, it also holds many dangers that we are exposed to, and that can affect our personal lives and everything related to it. Nowadays, companies all around the world have changed their traditional administrative systems and have evolved them into more technological and modern ones that adapt with todays world. However, these companies have become the key target of cyber-attackers that tend to perpetrate an attack in order to obtain any benefit from it.

Another big problem is the fact that cyber-attacks do not always have the same structure, which makes them more difficult to detect. That's why this report is focused on cyber-attacks, and more specifically a more complex type of attack, the multi-stage attack. Through this report, many ways to detect and understand this type of attacks will be discussed, and also different prevention mechanisms will be exposed.

II. Concepts

A multi-stage attack is a type of cyber-attack that is launched in multiple sequencial stages, as we can imply from the name, and its main objective is to maintain long-term access to the victim's network. Each one of the stages within the entire attack can be completed by executing different actions that are not necessarily malicious, but necessary for a successful completion. Unlike single-step attacks, the time between the execution of each stage can be hours, days or months, making the detection of multi-stage attacks extremely challenging [17].

It's known that most multi-stage attackers do not give up easily and persist until the attack is fully executed, because after the completion of each stage of the attack, they obtain more resources that can later be used to infiltrate successfully into the targeted system.

There are two main reasons why attackers decide to proceed with multi-stage attacks [13]. First, the targets chosen are usually major businesses and organizations, which means that it would be almost impossible to complete a successful attack by using a normal single-step attack, due to the complex network topology and security that this type of targets usually have. Second, if the attack is completed in more than one stage, it is more difficult for the victim to identify if an attack is happening inside its network, because some of the stages can be executed without being a threat to the targeted system.

The execution of a multi-stage attack starts by identifying the weaknesses in a potential target, and once this is completed, the real attack can take place. Once the target is selected, the attacker creates a Point of Entry (PoE), and once inside the targeted network a communication channel with the attacker should be established, so the rest of the attack can continue with no interference. This initial stage of the attack typically includes an initial dropper file, which can contain any type of malware that has the main purpose to download another file from the Internet, which will be useful to continue with the rest of the attack [2].

Multi-stage attacks have become a big challenge to face in recent years, as it is very difficult to detect them in their early stages due to the novel techniques and mechanisms used to perpetrate the attack, which means that once they are detected it may be too late to stop them on time [16].

We can briefly mention the most relevant challenges faced when trying to detect a multi-stage attack, which were described in [13]:

- The most common problem when trying to detect multi-stage attacks is that current Intrusion Detection Systems (IDSs) analyze network traffic information looking for signatures of known cyber-attacks, when they should also be able to analyze the context in which the systems operate [18].
- Multi-stage attacks can be executed with no specific order, so its complexity is major than the complexity of any other type of attack.
- Even though some stages can seem harmless, in reality they can be malicious.
- Because on how some stages are deployed or configured to be executed, the detection of an attack can be more complicated.
- In order to avoid recognition, attackers can perform irrelevant actions in the middle of the attack.
- Sometimes, alerts indicating a threat can be false positives, or contrarily, false negatives.
- And finally, since this type of attack is very novel, there are not many resources available for the analysis of multi-stage attack. Therefore, the existing research is not really relevant due to the lack of previous information.

A. Types of multi-stage attacks

We can face two different types of multi-stage attacks. The first type tries to infect as many machines within the targeted network as possible, while the other tries to reach a specific target after executing different intrusion steps [5].

III. Detection

A. Detection approaches

We can start by discussing about the five detection approaches presented in [13], with which we can identify a multi-stage attack:

1. *Similarity-based:* this approach proposes the construction of different attack scenarios based only on the similarity between each stage composing the attack, as we can imply from the name. In other words, similar alerts can be related to the same origin, and therefore may belong to the same scenario.
2. *Causal correlation:* this approach focuses on the main structure of multi-stage attacks and the relationship between each one of its stages. Previous stages can give some clues of the ones that follow, and a causal scheme can be constructed from this entire relationship.
3. *Structural-based:* this approach projects incoming traces to a model of the targeted network, where the next stages of ongoing attacks can be predicted, and this prediction relies on the hypothesis of posible attack paths.
4. *Case-based:* this approach relies on detecting multi-stage attacks based only on well-known attack scenarios.
5. *Mixed:* this approach follows more than one of the already described approaches.

B. Detection methods

As we mentioned before, we can notice that the complexity of cyber-attacks has increased exponentially in the last years, that is why new IDSs need to detect cyber-attacks not only by looking into network traffic information, but also from the context available within the entire detection process. **Fuzzy Cognitive Map** (FCM) [1] is one of the only available methods that provides the capability of analyzing contextual information to detect an attack. It incorporates the Pattern-of-Life (PoL) model into the detection process and uses it to improve the methods normally used by any IDS to detect any evidence of an outgoing attack [19].

Machine learning has also been used to train datasets so they can help identifying the relations between different stages of an attack, and use those results to predict the probabilities of an upcoming individual stage [1].

Another mechanism commonly used to detect multi-stage attacks is the implementation of **attack graphs**, which have been proposed as a method to look out for vulnerabilities within a network, in order to understand the detection of this type of attacks [5]. However, they often require extensive modeling resources, which is time consuming and vulnerable to errors due to the quadratic complexity that this method usually has.

In [9], **Scenario Graphs** are described as an implementation to detect multi-stage attacks. With this method, an IDS alerts from different events occurring in a network, to then comprise them into groups of alerts, usually called exploits, in order to create a complete attack scenario with the relationship between each exploit. The benefits of applying this approach, described in [10], are:

- Real time warnings, since the scenarios constructed provide the necessary information to prevent a multi-stage attack from happening.
- The method provides means to detect stealthy stages, because it helps recognizing the objective of each stage, which can help predicting what the next stage of the attack might be. Once the goal of a stage is recognized, it is easier to predict the overall attack path [20].
- Since it uses a graph-based approach to construct attack scenarios, it takes advantage of different graph-based techniques that contribute to solving the problem successfully.

An interesting detection method is the **Intrusion Kill Chain (IKC) model** [2]. This method facilitates the identification of multi-stage attacks by following the IKC seven-phase model that an attacker generally follows to carry out an attack. The IKC phases are:

1. Information gathering: in this first phase the attacker selects its targets and collects any relevant information for the attack.
2. Weaponization: the main objective of this phase is the development of malicious code that can be delivered in payloads, like pdfs and docs, which will later infect the targeted machine.
3. Delivery: as we can imply, the main goal of this phase is to deliver the infected payload into the target.
4. Exploitation: in this phase, the goal is to execute the malicious code using the vulnerabilities of the target.
5. Installation: in order to maintain the persistence of the attacker within the target, Remote Access Trojan's (RAT) are generally executed in this phase.
6. Command and control (C2): the goal of this phase is to create a communication channel, known as C2 server, between the attacker and the machine, so the attacker can control the malware with no interference.
7. Actions: in this last phase, the attacker performs different actions in order to achieve its final objectives. We should be aware that if any of the past phases are not completed successfully, this phase can't be successful either.

So, by following the IKC model, we could be able to break the attack by interfering any of the seven phases. Breaking the attack at an early stage can stop the multi-stage on time [2].

C. Detection methods in IIoT

This section focuses mainly on multi-stage attacks directed to machines and networks related to Industrial

Internet of Things (IIoT). Even though executing an attack related with Internet of Things (IoT) may seem useless, it's pretty common nowadays.

That's why [7] proposed a bidirectional long and short-term memory (B-LSTM) network based on multi-feature layers, which can effectively detect multi-stage attacks based on previous registered data. The good thing about this method is that the results have shown a lower false positive and false negative rate than in other existing models, which means its more accurate and credible [21].

IV. Defence

The best way to deal with any type of cyber-attack is by preventing it from happening than by detecting it while its being executed, because in most cases it could be too late to stop it. The most common defense mechanism employed against multi-stage attacks is discovering any existing vulnerabilities within the network and develop the corresponding fixes to eliminate them [5]. However, this process can be tedious and time consuming, so if any vulnerability is present within the network, it is necessary to develop an effective defense plan able to respond to any intrusion on time.

There are other defense mechanisms available for us to implement inside of our networks, so this way we can prevent any multi-stage attack from happening. Some of them were described in the research papers used to develop this report, so they will be summarized in the following paragraphs.

Reinforcement learning is proposed in [5] as a defense mechanism against multi-stage attacks. This subclass of machine learning, has been increasingly applied in Active Cyber Defense (ACD), and it can be applied as a learning algorithm that helps reconfigure platforms in order to defend against this type of attacks.

Thompson sampling–based reinforcement learning algorithms, described in [5], can also be applied effectively over specific vulnerabilities in order to defend the system against multi-stage attacks, and the success of the algorithm has been verified in different simulations based on already perpetrated real-life attacks.

SandBlast Threat Emulation, described in [4], is a useful mechanism that helps protecting networks against unknown threats attached in web downloads. This tool detects malware at its initial phase, before penetrating the network, and quickly runs the suspicious files in a virtual environment in order to discover malicious behavior before attackers can perpetrate the real attack into the system.

Finally, **Layered Security Architecture** [2] has been proposed as a useful way to protect a network from multi-stage attacks. Since the detection of a complex attack can be difficult, if we put more obstacles in front of the attacker, he will need to spend more time finding resources to be successful on his attack. This way attacks can be prevented from happening since the aforementioned IKC phases would have to be executed every time the attacker encounters a new layer inside the targeted system [24-26].

So, if we decide to work with the described architecture, the final topology should fulfill the following requirements [2] in order to be fully effective:

- The only way possible to access to a layer should be through the immediately external layer. If this is correct, the attacker will first have to attack directly into a layer in order to get access to the next one.
- If this first requirement is fulfilled, the attacker will have to start the attack from the first external layer, making it harder for him to achieve its final goal [22].
- The probability of finding common susceptibilities in each layer should be very low, because the main idea of applying this detection method is too minimize the knowledge the attacker has over each one of the layers, so this method should force the attackers to find more information and tools in order to bypass each layer.

V. Real Life Examples of Multi-Stage Attacks

At this point of the report we fully understand how multi-stage attacks work, who they are usually targeted to, how to detect them and how to prevent them from happening. But our last point is about real-life examples of multi-stage attacks that have occurred in the recent years.

Common examples of multi-stage attacks are those that initiated using a video file. In [12] it is proposed a method of detecting multi-stage attacks with the help of API calls and antivirus tools. Even though antivirus may seem useful for detecting this type of attack, in reality these tools are not capable of analyzing malicious content attached in images and video files. So, attackers usually spread malicious files embedded in movies or mp3 files through torrents and other free download sites [23].

Another multi-stage attack occurred in 2019 [4], when a campaign that targeted the clients of a major bank in Kazakhstan was uncovered. This campaign used an infected file hosted on the website of the financial institution to spread the malicious code. Once executed the file, a multi-stage attack started and eventually downloaded and executed a malware, providing the attackers a free entry inside of the bank's system [27-30].

Now related to IIoT [7], discovered in 2010, Stuxnet is one of the most famous examples of multi-stage attacks. It is known for infecting the wireless and USB devices of the employees inside the targeted organization, and then use them to spread the malicious code into the network. Once the network is compromised, the attackers are able to collect a large amount of information, and the most amazing part is that they can stay inside the organization's network without being detected for months, until the virus arrives to the main server and the industrial equipment is completely attacked.

VI. CONCLUSION

Finally, we can affirm that cyber-attacks are a serious problem in today's world where everyone is always connected, especially major businesses and organizations that always need to be in connected to the internet, and have lots of information stored on private servers. We always need to be aware about the complexity of novel cyber-attacks, such as the one discussed in the report, and the way they have become a serious problem that has to be stopped in any way.

We must be extremely careful when facing this type of attacks and the stage in which they are at the moment we find them out, because, if we discover that the attack has been

executed successfully in more than one stage, the consequences can be devastating due to the complexity of the attack itself.

As we know now, there are many detection methods available for us to face multi-stage attacks. One of the most complete forms of detection is the Intrusion Kill Chain, which helps to identify an attack by following the IKC seven-phase model, that is based on the steps an attacker usually follows in order to perpetrate a successfully attack.

Finally, we found out that the best way to deal with any type of cyber-attack is by preventing it. We can protect our networks and machines by applying any of the discussed defense mechanisms, so that any existing vulnerability is not exploited to carry out an attack.

REFERENCES

[1] Aparicio-Navarro, F.J., Kyriakopoulos, K.G., Ghafir, I., Lambotharan, S. and Chambers, J.A. (2018) Multi-Stage Attack Detection Using Contextual Information. *IEEE Xplore* 1–9. Accessed November 24, 2022.

[2] I. Ghafir, V. Prenosil, J. Svoboda and M. Hammoudeh, "A Survey on Network Security Monitoring Systems," International Conference on Future Internet of Things and Cloud, Vienna, Austria, pp. 77-82, 2016.

[3] Bhatt, P., Yano, E.T. and Gustavsson, P. (2014) Towards a Framework to Detect Multi-stage Advanced Persistent Threats Attacks. *IEEE Xplore* 390–395. Accessed November 24, 2022.

[4] Chadza, T., Kyriakopoulos, K.G. and Lambotharan, S. (2020) Analysis of hidden Markov model learning algorithms for the detection and prediction of multi-stage network attacks. *Future Generation Computer Systems* 108, 636–649. Accessed November 17, 2022.

[5] S. Eltanani and I. Ghafir. "Coverage Optimisation for Aerial Wireless Networks." 2020 14th International Conference on Innovations in Information Technology (IIT). IEEE, 2020.

[6] I. Ghafir, V. Prenosil, M. Hammoudeh and U. Raza, "Malicious SSL Certificate Detection: A Step Towards Advanced Persistent Threat Defence," International Conference on Future Networks and Distributed Systems. Cambridge, United Kingdom, 2017.

[7] gmcdouga (2021) *Preventing multi-stage attacks with Check Point SandBlast Threat Emulation*. https://blog.checkpoint.com/2021/01/28/preventing-multi-stage-attacks-with-check-point-sandblast-threat-emulation/ Accessed November 17, 2022.

[8] Hu, Z., Zhu, M. and Liu, P. (2021) Adaptive Cyber Defense Against Multi-Stage Attacks Using Learning-Based POMDP. *ACM Transactions on Privacy and Security* 24 (1), 1–25. Accessed November 28, 2022.

[9] I. Ghafir, V. Prenosil, A. Alhejailan and M. Hammoudeh, "Social Engineering Attack Strategies and Defence Approaches." International Conference on Future Internet of Things and Cloud. Vienna, Austria, pp. 145-149, 2016.

[10] J. Svoboda, I. Ghafir, V. Prenosil, "Network Monitoring Approaches: An Overview," International Journal of Advances in Computer Networks and Its Security (IJCNS), vol. 5(2), pp. 88-93, 2015.

[11] M. Lefoane, I. Ghafir, S. Kabir, and I. Awan, "Machine Learning for Botnet Detection: An Optimized Feature Selection Approach". International Conference on Future Networks & Distributed Systems. Association for Computing Machinery, New York, NY, USA, 2021.

[12] Kour, R., Thaduri, A. and Karim, R. (2020) Predictive model for multistage cyber-attack simulation. *International Journal of System Assurance Engineering and Management* 11 (3), 600–613. Accessed November 24, 2022.

[13] M. Lefoane, I. Ghafir, S. Kabir, I. Awan, "Unsupervised Learning for Feature Selection: A Proposed Solution for Botnet Detection in 5G Networks", IEEE Transactions on Industrial Informatics, 2023.

[14] I. Ghafir, V. Prenosil, M. Hammoudeh, T. Baker, S. Jabbar, S. Khalid and S. Jaf, "BotDet: A System for Real Time Botnet Command and Control Traffic Detection," IEEE Access, vol. 6, pp. 1-12, 2018.

[15] Li, X., Xu, M., Vijayakumar, P., Kumar, N. and Liu, X. (2020) Detection of Low-Frequency and Multi-Stage Attacks in Industrial Internet of Things. *IEEE Transactions on Vehicular Technology* 69 (8), 8820–8831. Accessed November 28, 2022.

[16] Li, Z., Zhang, A., Li, D. and Wang, L. (2007) Discovering Novel Multistage Attack Strategies. *Advanced Data Mining and Applications* 45–56. Accessed November 25, 2022.

[17] A. Abdulhamid, S. Kabir, I. Ghafir and C. Lei, "Dependability of the Internet of Things: Current Status and Challenges," International Conference on Electrical, Computer, Communications and Mechatronics Engineering, Maldives, Maldives, 2022.

[18] I. Ghafir, J. Saleem, M. Hammoudeh, H. Faour, V. Prenosil, S. Jaf, S. Jabbar and T. Baker, "Security Threats to Critical Infrastructure: The Human Factor," The Journal of Supercomputing, vol. 74(10), pp. 1-17, 2018.

[19] Mathew, S., Britt, D., Giomundo, R., Upadhyaya, S., Sudit, M. and Stotz, A. (2005) Real-time multistage attack awareness through enhanced intrusion alert clustering. *IEEE Xplore* 1801–1806 Vol. 3. Accessed November 23, 2022.

[20] Mathew, S., Shah, C. and Upadhyaya, S. (2005) An alert fusion framework for situation awareness of coordinated multistage attacks. *IEEE Xplore* 95–104. Accessed November 29, 2022.

[21] M. Lefoane, I. Ghafir, S. Kabir and I. U. Awan, "Multi-stage Attack Detection: Emerging Challenges for Wireless Networks," International Conference on Smart Applications, Communications and Networking, Palapye, Botswana, 2022.

[22] I. Ghafir, V. Prenosil, and M. Hammoudeh, "Botnet Command and Control Traffic Detection Challenges: A Correlation-based Solution." International Journal of Advances in Computer Networks and Its Security (IJCNS), vol. 7(2), pp. 27-31, 2017.

[23] Mézešová, T., Sokol, P. and Bajtoš, T. (2020) Evaluation of Attackers' Skill Levels in Multi-Stage Attacks. *Information* 11 (11), 537. Accessed November 28, 2022.

[24] Nath, H.V. and Mehtre, B.M. (2015) Analysis of a multistage attack embedded in a video file. *Information Systems Frontiers* 17 (5), 1029–1037. Accessed November 29, 2022.

[25] Navarro, J., Deruyver, A. and Parrend, P. (2018) A systematic survey on multi-step attack detection. *Computers & Security* 76, 214–249. Accessed November 24, 2022.

[26] Shin, J., Choi, S.-H., Liu, P. and Choi, Y.-H. (2019) Unsupervised multi-stage attack detection framework without details on single-stage attacks. *Future Generation Computer Systems* 100, 811–825. Accessed December 2, 2022.

[27] I. Ghafir, M. Hammoudeh, V. Prenosil, L. Han and R. Hegarty, K. Rabie and F. J. Aparicio-Navarro, "Detection of Advanced Persistent Threat Using Machine-Learning Correlation Analysis," Future Generation Computer Systems, vol. 89, pp. 349-359, 2018.

[28] Takey, Y.S., Tatikayala, S.G., Samavedam, S.S., Lakshmi Eswari, P.R. and Patil, M.U. (2021) Real Time early Multi Stage Attack Detection. *IEEE Xplore* 283–290. Accessed November 29, 2022.

[29] Zhou, P., Zhou, G., Wu, D. and Fei, M. (2021) Detecting multi-stage attacks using sequence-to-sequence model. *Computers & Security* 105, 102203. Accessed November 25, 2022.

[30] M. Yazdi, S. Kabir, M. Kumar, I. Ghafir, F. Islam, "Reliability Analysis of Process Systems Using Intuitionistic Fuzzy Set Theory". In: Garg, H. (eds) Advances in Reliability, Failure and Risk Analysis. Industrial and Applied Mathematics. Springer, Singapore, 2023.