Early stage detection of cyber attacks

Bc. Martina Pivarníková

1Im, 2018 - 2019

Summary. Nowadays, systems around the world face many cyber attacks every day. These attacks consist of numerous steps that may occur over an extended period of time. We can learn from them and use this knowledge to create tools to predict and prevent attacks. In this paper, we introduce a way to sort cyber attacks to phases, which can help with the detection of each stage of cyber attacks. In this way, we will be able to detect the earlier stages of the attack. We propose a solution using machine learning algorithms to predict how the attack will proceed. We can use this information for more effective defense against cyber threats.

Keywords: cyber attack, attack modeling, early stage detection, kill chain

1 Introduction

Due to the constant development of cyber threats, various defense solutions need to be constantly improved. In addition to developing prevention systems, it is also necessary to focus on detection systems that help to obtain information about threats and attacks. Detecting malicious actions is one of the most important cyber security issues. Intrusion detection responds to the detection of specific patterns or anomaly observations. Nowadays, however, we need to preventively anticipate upcoming harmful activities, so that we can react to them and prevent an attack in time until it causes some harm. Such a task is called attack projection. Attack prediction research is not as prominent as its detection. Therefore, it needs to be devoted to, because it is beneficial for the entire field of cyber security. In order to predict attacks, it is necessary to examine how they proceed and what steps are being taken. This data can be used to continually improve the systems to detect each phase of the attack. In this way, it will be possible to detect the earlier stages of the attacks and predict how they will proceed. To summarize, the research challenges to be addressed are:

How can we predict the next move of an attacker or next steps of the attack? Early detection and prediction of cybersecurity incidents, such as attack is a challenging task. The threat landscape is constantly evolving and even with the usage of intrusion detection systems, advanced attackers can spend more than 100 days in a system before being discovered [1]. After the detection of a security incident, we need to determine, what steps will attacker make next and how the attack will proceed. This is very important because we can stop the attacker in time, so he cannot do as much damage.

How can we distinguish and sort attack steps? It is important to learn from existing attacks so that we can develop tools to find out if such an attack has been repeated. Attack modeling is an intrusion-based methodology that allows one to focus on the different stages of an attack. It is aimed at focusing on different phases of attack. By implementing tools to foil attacks at their various stages and identifying attacks at different stages, detective and preventive measures can be taken to ensure that similar attacks are detected. It is important to have a layered model to ensure that if one of the defense systems is bypassed, there is another defense line to protect your organization's assets. That is why we need to establish a multi-layered model of cyber attacks.

How can these predictions help with attack mitigation or preparing for upcoming security threat? In recent years, the demand is not for only being alerted of a security incident. Prevention of the attack altogether has become a necessity. The highest priority in computer security is to prevent an attack and stop the attacker from doing damage. If the path of an attack can be predicted, one has the ability to prevent attacks at every phase. By looking at a survey of the technology, from host to the network level, one will have an opportunity to study tools or solutions that can be used in protecting against these threats. There exist many prevention methods, able to stop attacks in progress.

The first part of this paper analyses current approaches to modeling cyber attacks. Based on this analysis, it is possible to choose the most appropriate solution for separating cyber attacks into stages. This can later help in attack prediction. We will look into existing approaches in prediction methods next. Subsequently, we will present the dataset we will work within this paper. After that, we will introduce our own cyber attack model, which contains four main stages of an attack. We will then try to assign security incidents to the proposed phases. This will support us in determining the prediction method of a cyber attack. It is also needed to be established, what prediction techniques will we use in order to maximize the success rate of attack prognostication.

1.2 Related work

In this section, we will focus on existing approaches that are related to our work. We divided them into Cyber attack modeling and Attack prediction methods. We chose this division because the first objective of this thesis is cyber attack modeling. The second objective is implementing the system for early-stage cyber attack detection.

1.2.1 Cyber attack modeling

In order to anticipate how the cyber attack will continue, we need to document the behavior of the attackers and provide a description of attack steps. The sample model of cyber attack stages was given in the paper by **Bou-Harb et al. [2]**. The anatomy of a cyber attack shows that cyber scanning plays a significant role.

In 2011, **Lockheed Martin Corporation** in **[3]** introduced the term Kill Chain, which models the structure of a cyber attack and intrusion into the computer system. They defined various stages of an attack and have designed a reporting framework managed by this chain for the analysis, detection, and prevention of cyber attacks and intrusion. There are seven stages of traditional kill chain model - reconnaissance, weaponization, delivery, exploitation, installation, Command and Control and act on the objective. This model is based on the assumption that attackers will seek to penetrate the computer system in a sequential and progressive way.

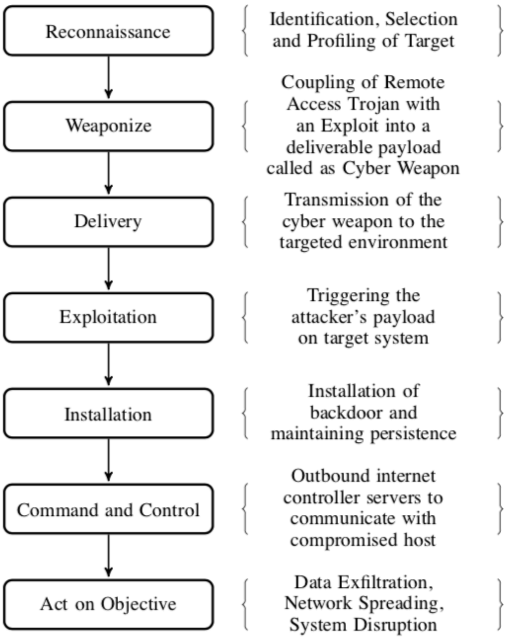

Reconnaissance
Identification, Selection and Profiling of Target
Weaponize
Coupling of Remote Access Trojan with an Exploit into a deliverable payload called as Cyber Weapon
Delivery
Transmission of the cyber weapon to the targeted environment
Exploitation
Triggering the attacker's payload on target system
Installation
Installation of backdoor and maintaining persistence
Command and Control
Outbound internet controller servers to communicate with compromised host
Act on Objective
Data Exfiltration, Network Spreading, System Disruption

Figure 1. Phases of Cyber Kill Chain [4]

After the introduction of the Kill Chain model, many researchers worked with it, because of its complexity and adaptability. **Greene** in **[5]** proposed an alteration to look at internal cyber kill chain stages. Though, this model lacks the important factor of analyzing the network defenses in a layered approach. Network perimeter security does an important job of holding back an excess of network-based threats. For example, illegitimate SSL connections.

Laliberte in **[6]** proposed a modified cyber kill chain, where the weaponization stage is removed and the lateral movement is introduced after the CnC stage. This highlights the horizontal movement of the attack to gain access to the targeted assets with the use of intermediary nodes. However, many advanced threats perform lateral movement using multiple command and control communications. Therefore, this model lacks a holistic approach in addressing the variety of threats altogether.

Khan et al. in **[7]** introduced a new concept - cognitive cyber security model. It is an adaptive method of examining data using machine learning, natural language processing, and artificial intelligence. They proposed a model, where kill chain stages were combined into the following four categories shown in Figure 2. First one, is reconnaissance for the exploitation of security weakness (R). The second one is delivery (D), third is developing the persistence to hide below the security radar using polymorphic and metamorphic behavior (P). The last one is command and control communications from the network and lateral movement within the network using endpoints/computing nodes (CnC). A cognitive time series of the suggested model is shown conceptually. If the time series is separated into N time steps, then each step establishes a four phase cycle. An object could be a network trace, server logs, and packet captures. Furthermore, the same object can be analyzed at multiple time steps but all the four stages are contemplated concurrently at each time step.

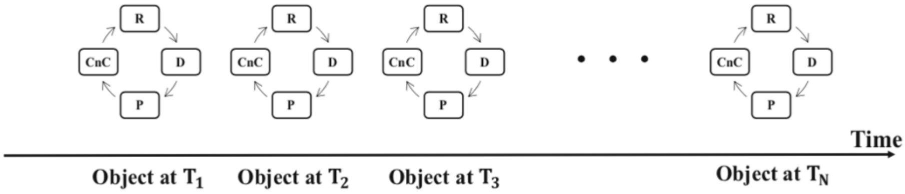


Figure 2. Proposed cognitive analytical kill chain model for simultaneous analysis of data [7]

Zhou et al. in **[8]** expanded the cyber kill chain model to improve it. Therefore, it can be applied to industrial control systems to ensure that defenders in industrial control can learn the attackers' attack paths. They can rationally allocate security resources, take adequate security measures and make a risk management choice. They analyzed the difference between the attack on the industrial control system and the traditional computer system. In this paper, a kill chain model for industrial control systems was presented. It includes external kill chain, which is used to penetrate the corporate network, the internal kill chain, that is used to gain access to industrial control systems and Industrial control system (ICS) kill chain used to implement the final attack of a specialized production process.

Hahn et al. in **[9]** have introduced a new approach to understanding cyber attacks and related risks for cyber systems. Their framework consists of two elements, a three-layered logical model and a reference architecture for cyber-physical systems and a model of attacks, which is referred to as kill chain. The layered architecture provides a base for studying how a causal chain associated with cyber perturbations can be traced to physical perturbation. The proposed framework offers a new approach to the comprehensive exploration of attack elements, including the targets of attackers, cyber exploitation, control-theoretic properties, and physical system properties. Their goal was to use the framework as a means to derive the security features of the cyber-physical system and to enumerate the principles of designing systems that are resistant to cyber attacks.

Authors	Model	Description
Bou-Harb et al. [2].	Cyber Scanning, Enumeration, Intrusion attempt, Elevation of privilege, Perform Malicious Tasks, Deploy Malware/Backdoor, Delete Forensics Evidence and Exit	Non-attribution anomaly detection approach
Hutchins et al. [3]	Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control (C&C), Act on Objectives	Introduction of kill chain model
Greene [5]	Internal kill chain steps	Alteration to look at internal cyber kill chain stages
Laliberte [6]	Reconnaissance, Delivery, Exploitation, Installation, Command and control, Lateral movement, Actions on objectives	Modified cyber kill chain
Khan et al. [7]	Reconnaissance, Delivery, Persistence to hide below the security radar using polymorphic and metamorphic behavior, Command and Control	Cognitive Cyber Security concept
Zhou et al. [8]	External kill chain, Internal kill chain, ICS kill chain	Kill chain applicable to industrial control systems
Hahn et al. [9]	Three-layered logical model and a reference architecture for cyber-physical systems and a kill chain model	New approach to the comprehensive exploration of attack elements - targets of attackers, cyber exploitation, control-theoretic properties, and physical system properties

Table 1. Summary of cyber attack modeling methods

1.2.2. Attack prediction methods

A large number of cyber attack prediction methods is using discrete models, using graph models, such as attack graphs, Bayesian networks or Markov models.

In 1998, an attack graph was introduced by **Swiler and Phillips [10]**. It is a graphical representation of an attack scenario. This has become a popular method of a formal description of attacks. It has become a foundation for other approaches, e.g. methods using Bayesian networks, Markov models and game-theoretical methods. An attack graph is a tuple $G = (S, r, S_0, S_s)$, where S is a set of states, $r \subseteq S \times S$ is a transition relation, $S_0 \subseteq S$ is a set of initial states, and $S_s \subseteq S$ is a set of success states [11]. Edges between states describe the potential actions of an attacker. They can be weighted, to represent the probability that the attacker will choose the action. If he gets from the initial state to any of the success states, the attack is successful.

Cao et al. [12, 13] proposed another variant of attack graph - factor graph. It is a probabilistic model that consists of random variables and factor functions. he authors compare it to Bayesian networks and Markov random fields. They evaluate the use of factor graph for predicting attacks over a large dataset of real security incidents (several years of reports) with an accuracy of 75 %.

RTECA (Real Time Episode Correlation Algorithm) was proposed in 2014 by **Ramaki et al. [14].** It can be used for multi-step attack scenarios detection and prediction. They explain the theoretical and functional implications of creating such a tool. Although they propose leveraging attack graph, the authors widely use causal correlations in their method.

Wu et al. [15] used another attack prediction method using Bayesian networks. These methods are related to approaches based on attack graphs because a Bayesian network is built from an attack graph. The distinct characteristic of Bayesian networks are the conditional variables and probabilities that are considered in the model.

A Bayesian network is a probabilistic graphical model that represents the variables and the relationships between them. The network is a directed acyclic graph (DAG) with nodes as the discrete or continuous random variables and edges as the relationships between them. Formally, let $G = (V, E)$ be a DAG, and let $X = (X_v)vV$ be a set of random variables indexed by V. A Bayesian Network consists of a set of variables and a set of direct edges between variables. Each variable has a finite set of mutually exclusive states. The variable and direct edge form a DAG. To each variable A with parents $B1, B2, ..., Bn$, there is attached a conditional probability table $P(A|B1, B2, ..., Bn)$ [16].

A real-time alert correlation and prediction framework was introduced by **Ramaki et al. [17]**. The framework has two modes, online and offline. In the online mode, the most presumable next step of the attacker is predicted according to the Bayesian attack graph. In the offline mode, the Bayesian attack graph is built from low-level alerts. The authors used the DARPA 2000 dataset for research. The accuracy of prediction was observed to be increasing with the length of the attack scenario. Thus, precision varied from 92.3% when processing the first attack step to 99.2% when processing the fifth attack step.

Okutan et al. [18] involved signals unrelated to the target network into the attack prediction method based on the Bayesian network. The signals are mentions of attacks on Twitter or the current number of attacks from Hackmageddon [19]. As was shown in results, prediction accuracy differs from 63 % to 99 %, which makes it a promising method.

Another widely used approach to predicting attacks is using Markov models. These methods were introduced along with approaches based on attack graphs and Bayesian networks in late 2000'. A complex framework for alert correlation and prediction was proposed by **Farhadi et al.** [**20**]. Sequential pattern mining was used to extract attack scenarios, which are then represented using a Hidden Markov model that is used for attack plan recognition. Markov models operate well in the presence of unobservable states and transitions. Thus, they are not dependent on possessing complete information. This allows successful attack prediction, even if some attack stages were undetected or absent.

Sendi et al. [21] proposed a method of real-time intrusion prediction using Hidden Markov Models. The prime interest in this paper is multi-step attacks. An empirical evaluation shows how their approach can predict multi-step attacks, which is particularly useful for preventing the attacker from gaining control over more and more hosts in the computer network.

Shin et al. [22] in 2013 introduced a probabilistic approach for network-based intrusion detection system (IDS, APAN), that uses a Markov chain to model unusual events in the network traffic and to predict intrusion. Opposed to other methods based on Markov models, this method processes network anomalies and is not intending to predict the next move of an attack like other model-checking approaches.

Authors	**Approach/Model**	**Advantages and limitations**
Swiler and Phillips [10]	Attack graph	The first proposed methods
Cao et al. [12, 13]	Attack graph	75 % accuracy, factor graph
Ramaki et al. [14]	Attack graph	95 % accuracy
Wu et al. [15]	Bayesian network	Only model extensions
Ramaki et al. [17]	Bayesian attack graph	92.3–99.2 % accuracy, real-time
Okutan et al. [18]	Bayesian network	63%–99% accuracy, non-conventional signals
Farhadi et al. [**20**]	Hidden Markov model	81.33 %–98.3 % accuracy, data mining, illustrative example of a real-time attack projection framework
Sendi et al. [21]	Hidden Markov model	Prediction of next step in multi-step attack
Shin et al. [22]	Markov chain	Improving intrusion detection by predictions

Table 2. Summary of cyber attack prediction methods

2 Approach and methods

In this chapter, we will introduce how the data we work with look like. We will describe a dataset that contains real attacks on computer systems. The cyber attack prediction method will learn on this dataset. Then we will introduce approaches to modeling cyber attacks and present our own model. We will describe all of his phases in detail.

2.1 Dataset

For this paper, we work with "Intrusion Detection Evaluation Dataset (CICIDS2017)" dataset. It includes benign and the most common attacks, which matches the real-world data (PCAPs). It also includes the results of the network traffic analysis using CICFlowMeter with labeled flows based on the time stamp, source, and destination IPs, source and destination ports, protocols and attack (CSV files). The data capturing period started at 9 a.m., Monday, July 3, 2017, and ended at 5 p.m. on Friday, July 7, 2017, for a total of 5 days. Monday only includes normal traffic. The implemented attacks include Brute Force FTP, Brute Force SSH, DoS, Heartbleed, Web Attack, Infiltration, Botnet and DDoS. They have been executed both morning and afternoon on Tuesday, Wednesday, Thursday and Friday [23]. We will now describe captured traffic and cyber attacks from each day of this dataset.

Monday, July 3, 2017

- Benign (Normal human activities)

Tuesday, July 4, 2017

Within this day, Brute Force FTP and Brute Force SSH attacks were performed. We can see the detailed description next.

- **Brute Force**
    - FTP-Patator (9:20 – 10:20 a.m.)
    - SSH-Patator (14:00 – 15:00 p.m.)
  - **Attacker**: Kali, 205.174.165.73
  - **Victim**: WebServer Ubuntu, 205.174.165.68
    (Local IP: 192.168.10.50)
- **NAT Process on Firewall:**
  - **Attack**: 205.174.165.73 -> 205.174.165.80 (IP Valid Firewall) -> 172.16.0.10 -> 192.168.10.50
  - **Reply**: 192.168.10.50 -> 172.16.0.1 -> 205.174.165.80 -> 205.174.165.73

Wednesday, July 5, 2017

On Wednesday, multiple Dos/DDos attacks were executed in the morning. In the afternoon, Heartbleed vulnerability was used to execute the attack. We can see the detailed description next.

- **DoS / DDoS**
- **DoS slowloris (9:47 – 10:10 a.m.)**
- **DoS Slowhttptest (10:14 – 10:35 a.m.)**
- **DoS Hulk (10:43 – 11 a.m.)**
- **DoS GoldenEye (11:10 – 11:23 a.m.)**
  - **Attacker**: Kali, 205.174.165.73
  - **Victim**: WebServer Ubuntu, 205.174.165.68
    (Local IP 192.168.10.50)

- **NAT Process on Firewall:**
    - **Attack:** 205.174.165.73 -> 205.174.165.80 (IP Valid Firewall) -> 172.16.0.10 -> 192.168.10.50
    - **Reply:** 192.168.10.50 -> 172.16.0.1 -> 205.174.165.80 -> 205.174.165.73
- **Heartbleed Port 444 (15:12 - 15:32)**
    - **Attacker**: Kali, 205.174.165.73
    - **Victim**: Ubuntu12, 205.174.165.66 (Local IP: 192.168.10.51)
- **NAT Process on Firewall:**
    - **Attack**: 205.174.165.73 -> 205.174.165.80 (IP Valid Firewall) -> 172.16.0.11 -> 192.168.10.51
    - **Reply**: 192.168.10.51 -> 172.16.0.1 -> 205.174.165.80 -> 205.174.165.73

Thursday, July 6, 2017

This day includes multiple web attacks, such as cross-site scripting and Sql injection. Then, int the afternoon, an infiltration was performed. We can see the detailed description next.

- **Web Attack – Brute Force (9:20 – 10 a.m.)**
- **Web Attack – XSS (10:15 – 10:35 a.m.)**
- **Web Attack – Sql Injection (10:40 – 10:42 a.m.)**
    - **Attacker**: Kali, 205.174.165.73
    - **Victim**: WebServer Ubuntu, 205.174.165.68
      (Local IP: 192.168.10.50)

- **NAT Process on Firewall:**
    - **Attack**: 205.174.165.73 -> 205.174.165.80 (IP Valid Firewall) -> 172.16.0.10 -> 192.168.10.50
    - **Reply**: 192.168.10.50 -> 172.16.0.1 -> 205.174.165.80 -> 205.174.165.73
- **Infiltration – Dropbox download**
- **Meta exploit Win Vista (14:19 and 14:20-14:21 p.m.) and (14:33 -14:35)**
    - **Attacker**: Kali, 205.174.165.73
    - **Victim**: Windows Vista, 192.168.10.8
- **Infiltration – Cool disk – MAC (14:53 p.m. – 15:00 p.m.)**
    - **Attacker**: Kali, 205.174.165.73
    - **Victim**: MAC, 192.168.10.25
- **Infiltration – Dropbox download - Win Vista (15:04 – 15:45 p.m.)**
    - First Step:
        - **Attacker**: Kali, 205.174.165.73
        - **Victim**: Windows Vista, 192.168.10.8
    - Second Step (Portscan + Nmap):
        - **Attacker**: Vista, 192.168.10.8
        - **Victim**: All other clients

Friday, July 7, 2017

In the morning of this day, the ARES botnet was executed on computers. After that, a port scan was performed. In the afternoon, the DDoS LOIT attack was carried out. . We can see the detailed description next.

- **Botnet ARES (10:02 a.m. – 11:02 a.m.)**
    - **Attacker**: Kali, 205.174.165.73
    - **Victims**: Win 10, 192.168.10.15 + Win 7, 192.168.10.9 + Win 10, 192.168.10.14 + Win 8, 192.168.10.5 + Vista, 192.168.10.8
- **Port Scan**
    - **Firewall Rule on** (13:55 – 13:57, 13:58 – 14:00, 14:01 – 14:04, 14:05 – 14:07, 14:08 - 14:10, 14:11 – 14:13, 14:14 – 14:16, 14:17 – 14:19, 14:20 – 14:21, 14:22 – 14:24, 14:33 – 14:33, 14:35 - 14:35)
    - **Firewall rules off** (sS 14:51-14:53, sT 14:54-14:56, sF 14:57-14:59, sX 15:00-15:02, sN 15:03-15:05, sP 15:06-15:07, sV 15:08-15:10, sU 15:11-15:12, sO 15:13-15:15, sA 15:16-15:18, sW 15:19-15:21, sR 15:22-15:24, sL 15:25-15:25, sI 15:26-15:27, b 15:28-15:29)
    - **Attacker**: Kali, 205.174.165.73
    - **Victim**: Ubuntu16, 205.174.165.68 (Local IP: 192.168.10.50)
- **NAT Process on Firewall:**
    - **Attack**: 205.174.165.73 -> 205.174.165.80 (IP Valid Firewall) -> 172.16.0.10 -> 192.168.10.50
- **DDoS LOIT (15:56 – 16:16)**
    - **Attackers**: Three Win 8.1, 205.174.165.69 - 71
    - **Victim**: Ubuntu16, 205.174.165.68 (Local IP: 192.168.10.50)

This dataset was processed by SNORT intrusion detection system [24], which raised multiple alerts that matched described attacks. After that, the alerts were correlated – if there were two or more similar or the same alerts in one time window, and they have at least one common IP address (attacker's or victim's), they were aggregated into one hyper alert. They were afterward correlated – relationships between hyper alerts were established based on some properties, such as time window, IP addresses, ports, etc. These relations were weighted based on how much they were alike. After these methods, a directed weighted graph was made, where vertices are hyper alerts and the weighted edges are relations between them. From this graph, we can create all possible paths between vertices. It needs to be established, which paths are relevant – if they represent an attack. Then we need to determine, which type of attack it is. Therefore, the attacks will be represented by a directed weighted subgraph. This subgraph will be used as a base graph for cyber attack prediction methods using discrete models – Bayesian network or Markov model.

2.2 Cyber attack modeling

We considered using one of the three models for analyzing and using in our paper – Kill chain model [3], the model presented in [2], and Diamond model [25]. In the following text, we will describe them in detail.

Kill chain model

As was described before, the cyber kill chain model defines the path of a cyber attack. In this seven-layered model, each layer is critical for the evaluation of the attack. By studying the cyber kill chain is helpful for identifying cyber threats and it can also help with mitigation of the attack at any stage. Sooner the detection, the lesser damage will be done to the computer system.

In the first phase - **reconnaissance**, the attacker is gathering information about the potential target. A target can be a personal computer or a computer network. Reconnaissance can further be broken down to target identification, selection, and profiling. It mostly includes crawling World Wide Web such as internet websites, conferences, blogs, social relationship, mailing lists and network tracing tools to get information about target [26].

The next stage - **weaponization**, deals with designing a backdoor and a penetration plan. The attacker is using the information gathered from reconnaissance, so he can be able to successfully deliver the backdoor. Technically it is binding software/application exploits with a remote access tool (RAT). Weaponizing includes the construction of the following two components [4]:

1. **RAT (Remote Access Tool)** - a piece of software which executes on target's system and give remote, hidden and undetected access to the attacker
    a. Client - a piece of code which is delivered to the target, it executes and builds a connection to the Command and Control infrastructure of the RAT.
    b. Server - the other half of RAT which runs on the Command and Control server
2. **Exploit** - the part of weapon which helps the RAT to execute, it serves as a carrier for RAT and uses system/software vulnerability to drop and execute RAT.

After the malware payload has been developed and the backdoor to deliver the payload has been identified, the **delivery** stage is executed. The malware can be delivered either by sending a phishing email with a malicious attachment or by visiting a malicious website and downloading suspicious files. It can by also delivered physically, for example keeping infected files in removable files, such as USB. Moreover, malware can be delivered automatically by exploiting the weaknesses of the protocols and/or software [4].

After delivering the malicious code, the target completes the required user interaction and code executes at the target side. At the **exploitation** stage, the main step is triggering the exploit. The purpose of an exploit is to silently install/execute the payload.

Installation of remote access malware on the victim system allows an attacker to maintain persistence inside the environment. Advanced techniques are used by highly motivated attackers. They are trying to maintain persistence through by injecting code into windows applications, or even registry [26].

A significant part of the remotely executed cyber attacks is the **Command and Control (C&C)** system. C&C system is used to give remote covert instructions to compromised hosts. It also serves as a place where all data can be exfiltrated. Over the years, the design of C&C channels has evolved because of the exponential growth of defensive mechanisms, e.g. antiviruses, firewalls, IDSs, etc. [27]. There are three types of C&C infrastructure - Centralized Structure, Decentralized Structure, and Social Networks Based Structure.

The last stage is the **Act on Objectives**. After getting the communication structure with the target system, the attacker executes the commands. The used commands depend on the interest of attack. There are two types of attacks [28]:

1. **Mass attack** - the purpose of mass attack to get as many targets as possible.
2. **Targeted attacks** - more sophisticated, most of them are aimed to get confidential or secret information from the target system.

The model presented by Bou-Harb et al. [2].

The anatomy of the attack consists of steps displayed in Figure 3. The first step – **cyber scanning** is the same as the reconnaissance step in the kill chain.

Enumeration is defined as the process of extracting user names, machine names, network resources, shares and services from a system. In this stage, the attacker creates an active connection to the system and performs directed queries to gain more information about the target. The gathered information is used to identify the vulnerabilities or weak points in system security.

Intrusion attempt means that the attacker tried to perform an attack on the computer system, but it was not fully successful. But the attacker could find out some of the information of the target during this phase.

An **elevation of privilege** stage represents a type of network intrusion that takes advantage of programming errors or design flaws to grant the attacker elevated access to the network and its associated data and applications. The next two stages – **perform malicious task and deploy malware/backdoor** - are divided stage of kill chain - act on objectives. The last stage consists of **deleting forensic evidence and exit**.

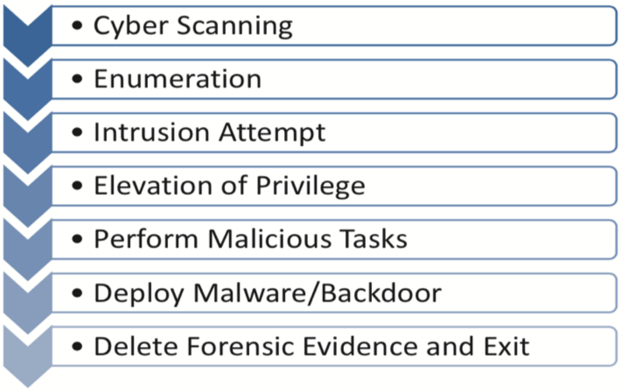

• Cyber Scanning
• Enumeration
• Intrusion Attempt
• Elevation of Privilege
• Perform Malicious Tasks
• Deploy Malware/Backdoor
• Delete Forensic Evidence and Exit

Figure 3. An anatomy of a cyber attack [2]

Diamond model

The Diamond model is one of the models for intrusion analysis. In this model, an attacker attacks a victim depending on two key motivations, instead of using a series of continuous steps such as kill chain. This model consists of four elements - adversary, infrastructure, capability, and the victim [25]. An adversary is an attacker who attacks a victim after analyzing their capability. The attacker starts with no knowledge of the capability of the victim. After analysis, he can find out, that he is more capable than the victim and then performs an attack. This model is important when dealing with high-level attackers such as those who have already obtained some control over the network. The attacker also analyses the infrastructure of his/her technical and logical ability to command and control a victim's network [29]. The diamond model can be seen in Figure 4. This model can also contain some of the meta-features such as timestamp, phases, result, directions, methodology, and resources.

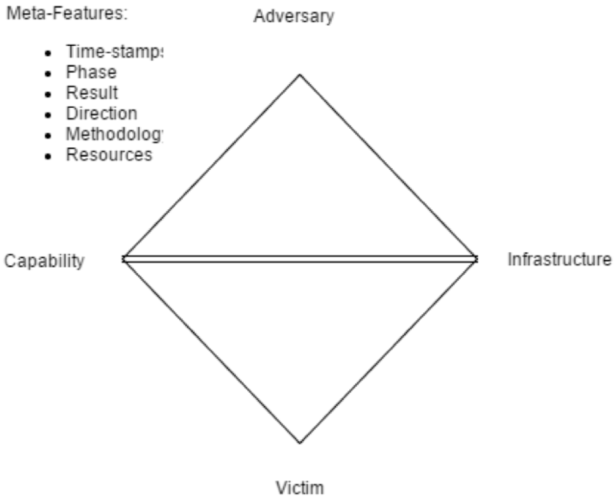


Figure 4. Diamond model [25]

Based on the analysis of the presented models it was concluded that neither of them met the requirements. That is why a new model needs to be developed. We introduce a hybrid model that includes four stages. This model can be seen in Figure 5.

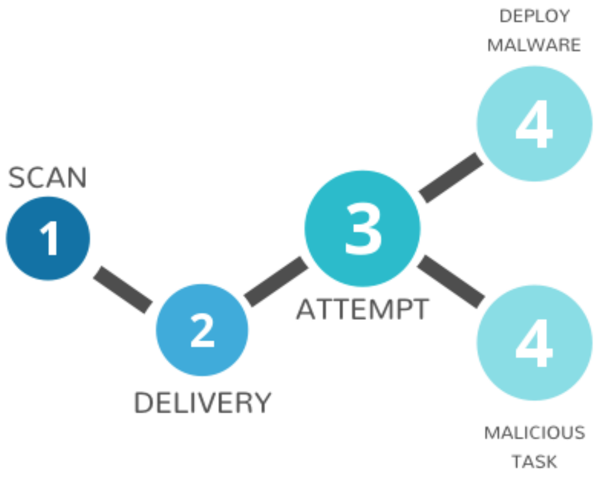


Figure 5. Cyber attack model

Scan

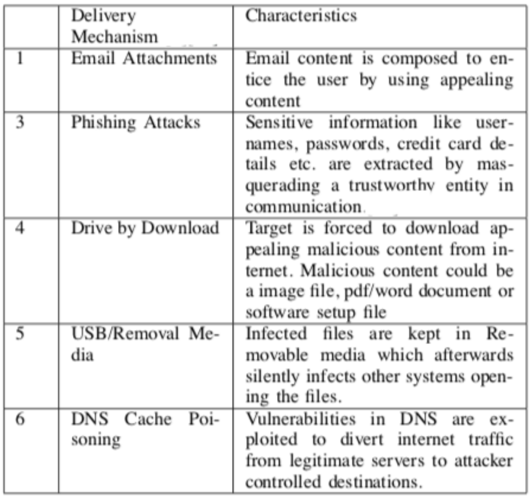
Cyber scanning is the first step in any sophisticated attack. This step is needed so the attacker can obtain information about his target, e.g. harvesting email addresses, login credentials or finding network vulnerabilities, etc. There exists a variety of methods that an attacker can use to achieve this goal. There are two types of scanning techniques - passive and active.

Passive scanning is an attempt to gain information about targeted computer systems and networks without actively engaging with the systems [30]. This can be performed by looking up the information about employees on the company website. These can be email addresses, personal social media accounts or phone numbers. LinkedIn and other social media networks can store employee information. That can help an attacker identify their potential goal. Also, social media accounts of employees can provide information about technologies used by the company. After finding out enough information about a victim, the possibility of success in social engineering increases. Passive scanning is the most difficult thing to detect from the perspective of Intrusion Detection Systems.

Active scanning is an attack in which an attacker engages a targeted network to gain information about vulnerabilities [30]. If an attacker is using an automated tool for network scanning, the IDS is likely to detect it and raise an alert. Performing active scanning is very valuable in determining any vulnerabilities that can be used. Network probing can be detected by correlating of logs over a period of time. Therefore, it can be determined who may be targeting the system. This paper will be focusing on network scanning captured by SNORT IDS. It can easily detect this type of stage. For example, if an attacker is using NMAP tool to obtain information about computer system (open ports or type of operating system), SNORT can recognize a large number of various types of incoming packets, therefore identify this type of scan. It will raise a `network-scan` type of alert after recognizing this stage.

Delivery

Delivery is the critical part of every cyber attack model because it is responsible for an effective cyber attack. In most of the cyber attacks, it is necessary to have some kind of user cooperation like downloading and executing malicious files or visiting malicious web pages on the internet. This stage presents a high risk for the attacker because delivery leaves evidence. Multiple delivery methods can be used, as we can see in Table 3. SNORT can detect malicious code by recognizing the transmission of executable code or suspicious strings in **network traffic.**



	Delivery Mechanism	Characteristics
1	Email Attachments	Email content is composed to entice the user by using appealing content
3	Phishing Attacks	Sensitive information like usernames, passwords, credit card details etc. are extracted by masquerading a trustworthv entity in communication
4	Drive by Download	Target is forced to download appealing malicious content from internet. Malicious content could be a image file, pdf/word document or software setup file
5	USB/Removal Media	Infected files are kept in Removable media which afterwards silently infects other systems opening the files.
6	DNS Cache Poisoning	Vulnerabilities in DNS are exploited to divert internet traffic from legitimate servers to attacker controlled destinations.

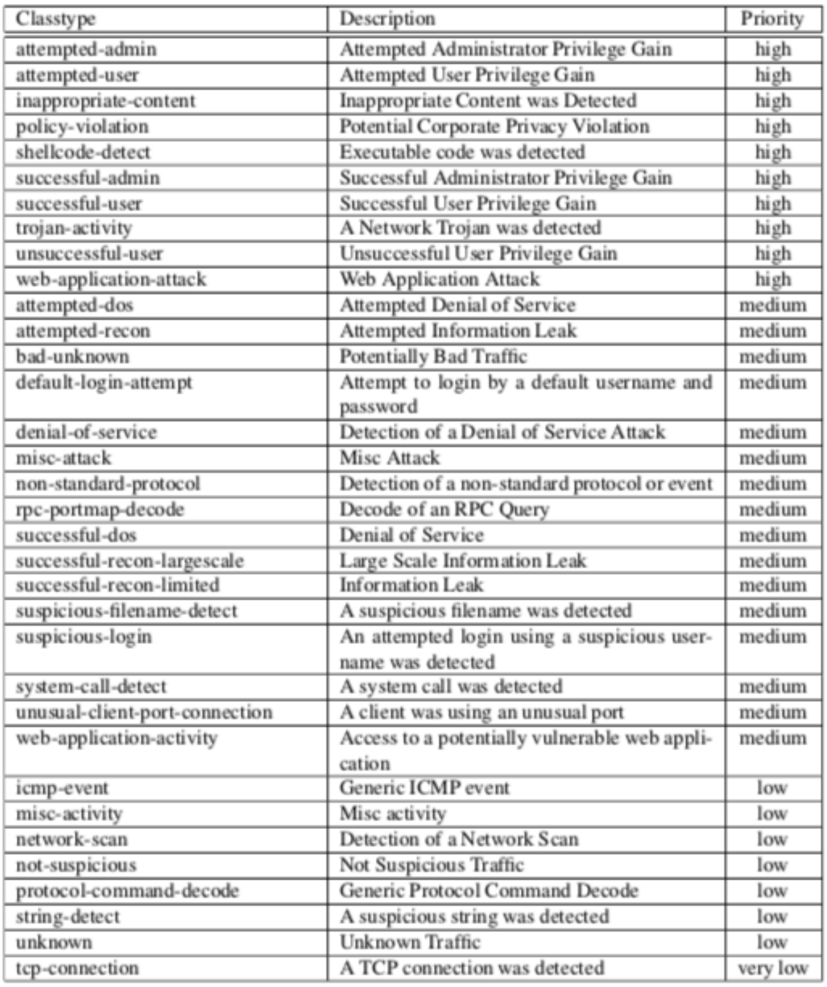
Table 3. Delivery Mechanisms [4]

Attempt

Intrusion detection means discovering that some entity, an attacker, has attempted to gain, or has already gained unauthorized access to the computer system. An intrusion attempt is a potential for a deliberate unauthorized attempt to enter either a computer, system or network to access information and manipulate information or render a system unreliable or unusable [31]. Intrusion attempts are basically experienced by victims, servers, networks, systems, and computers. These attempts can be discovered by intrusion detection systems. In the best case, it can be a false alarm, because detection systems can sometimes raise false positive alerts. In order to determine if this was the case, it is needed to look at the details of the alert. The second possibility is that the intrusion attempt came from an infected system on a local network. This alert can provide information about this system, for example, the address that caused the alert. It can be later checked for any malicious activity. The last possibility is that there was an attempt to attack from an outside local network, but it was blocked. But there is no way to determine if the attacker didn't obtain any information. Detection of intrusion attempt can be helpful in defending a network, for example blacklisting IP addresses or updating firewall configurations.

Deploy malware/Malicious task

This stage contains the last four stages in the Kill chain model. In this phase, the malware was successfully installed on a computer system, or an attacker has obtained rights on the targeted device and is performing some malicious action. It starts with exploitation, which is initiated by installing the malware inside the target computer. The malware or the attacker has the required access rights. If the malware is an executable file or the malicious activity is based on code injection or an insider threat, then the installation is not required. After the malware was installed, it will start communication with the command and control server, which can be an attacker's device, server, or even social media network web server. If the attacker has gained access to a targeted computer system, he will perform some malicious task, for example stealing private and intellectual data from the network.



Classtype	Description	Priority
attempted-admin	Attempted Administrator Privilege Gain	high
attempted-user	Attempted User Privilege Gain	high
inappropriate-content	Inappropriate Content was Detected	high
policy-violation	Potential Corporate Privacy Violation	high
shellcode-detect	Executable code was detected	high
successful-admin	Successful Administrator Privilege Gain	high
successful-user	Successful User Privilege Gain	high
trojan-activity	A Network Trojan was detected	high
unsuccessful-user	Unsuccessful User Privilege Gain	high
web-application-attack	Web Application Attack	high
attempted-dos	Attempted Denial of Service	medium
attempted-recon	Attempted Information Leak	medium
bad-unknown	Potentially Bad Traffic	medium
default-login-attempt	Attempt to login by a default username and password	medium
denial-of-service	Detection of a Denial of Service Attack	medium
misc-attack	Misc Attack	medium
non-standard-protocol	Detection of a non-standard protocol or event	medium
rpc-portmap-decode	Decode of an RPC Query	medium
successful-dos	Denial of Service	medium
successful-recon-largescale	Large Scale Information Leak	medium
successful-recon-limited	Information Leak	medium
suspicious-filename-detect	A suspicious filename was detected	medium
suspicious-login	An attempted login using a suspicious username was detected	medium
system-call-detect	A system call was detected	medium
unusual-client-port-connection	A client was using an unusual port	medium
web-application-activity	Access to a potentially vulnerable web application	medium
icmp-event	Generic ICMP event	low
misc-activity	Misc activity	low
network-scan	Detection of a Network Scan	low
not-suspicious	Not Suspicious Traffic	low
protocol-command-decode	Generic Protocol Command Decode	low
string-detect	A suspicious string was detected	low
unknown	Unknown Traffic	low
tcp-connection	A TCP connection was detected	very low

Table 4. SNORT alert classification [32]

Based on the proposed model, which contains four stages, alerts from intrusion detection system SNORT will be assigned into various phases. Raised alerts will be sorted based on their types to the proposed stages. We can see the categories with descriptions and priorities in Table 4. Then it can be determined, how are various attacks behaving in these phases. This will help in determining, how will the attack proceed once we get an alert of action, that belongs to earlier stages.

3 Conclusion

Because of the continuous threat of advanced cyber attacks, this work is based on the research of them. The first objective we need to look into is analysis, comparison, and processing of the current approaches to cyber attacks modeling. In this paper, we have summarized existing methods for cyber attack modeling and attack prediction approaches. The second objective of this thesis is creating a model data set from security events. We have presented and described "Intrusion Detection Evaluation Dataset (CICIDS2017)" dataset, which we will work with.

Design, implementation, and evaluation of the model for early-stage detection of cyber attacks is the third objective of this thesis. We have introduced our own model for cyber attack modeling. This model contains four stages, in which we will sort cyber security incidents. These incidents are alerts raised by SNORT intrusion detection system. After analyzing the mentioned incidents, we will implement an automatic system for classification of attack steps into stages. After that, we will determine what cyber attack prediction technique will we use in this paper. Next, we will implement a system for cyber attack prediction, which will be based on tracking the attack patterns that occurred in the used dataset.

References

1. *FireEye*. *Common vulnerability scoring system.*; Available from: https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf.
2. BOU-HARB, E., M. DEBBABI, and C. ASSI, *A systematic approach for detecting and clustering distributed cyber scanning*. Computer Networks, 2013. **57**(18): p. 3826-3839.
3. HUTCHINS, E.M., M.J. CLOPPERT, and R.M. AMIN, *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, in *Proceedings of leading issues in information warfare and security research*. 2011, Lockheed Martin Corporation.
4. YADAV, T. and A.M. RAO. *Technical aspects of cyber kill chain*. in *International Symposium on Security in Computing and Communication*. 2015. Springer.

5. GREENE, T., *Why the 'cyber kill chain'needs an upgrade*. Network World From IDG. Retrieved from: https://www.networkworld.com/article/3104542/security/why-the-cyber-kill-chain-needs-an-upgradesecurity-pros-need-to-focus-more-on-catching-attackers-aft.html, 2016.
6. LALIBERTE, M., *A new take on the cyber kill chain*. 2016, Sep.
7. KHAN, M.S., S. SIDDIQUI, and K. FERENS, *A cognitive and concurrent cyber kill chain model*, in *Computer and Network Security Essentials*. 2018, Springer. p. 585-602.
8. ZHOU, X., et al. *Kill Chain for Industrial Control System*. in *MATEC Web of Conferences*. 2018. EDP Sciences.
9. HAHN, A., et al., *A multi-layered and kill-chain based security analysis framework for cyber-physical systems*. International Journal of Critical Infrastructure Protection, 2015. **11**: p. 39-50.
10. SWILER, L.P. and C. PHILLIPS, *A graph-based system for network-vulnerability analysis*. 1998, Sandia National Labs., Albuquerque, NM (United States).
11. SHEYNER, O., et al. *Automated generation and analysis of attack graphs*. in *Proceedings 2002 IEEE Symposium on Security and Privacy*. 2002. IEEE.
12. CAO, P., et al. *Preemptive intrusion detection*. in *Proceedings of the 2014 Symposium and Bootcamp on the Science of Security*. 2014. ACM.
13. CAO, P., et al. *Preemptive intrusion detection: Theoretical framework and real-world measurements*. in *Proceedings of the 2015 Symposium and Bootcamp on the Science of Security*. 2015. ACM.
14. RAMAKI, A.A., M. AMINI, and R.E. ATANI, *RTECA: Real time episode correlation algorithm for multi-step attack scenarios detection*. computers & security, 2015. **49**: p. 206-219.
15. WU, J., L. YIN, and Y. GUO. *Cyber attacks prediction model based on Bayesian network*. in *2012 IEEE 18th International Conference on Parallel and Distributed Systems*. 2012. IEEE.
16. HUSÁK, M., et al., *Survey of attack projection, prediction, and forecasting in cyber security*. IEEE Communications Surveys & Tutorials, 2018. **21**(1): p. 640-660.
17. RAMAKI, A.A., M. KHOSRAVI-FARMAD, and A.G. BAFGHI. *Real time alert correlation and prediction using Bayesian networks*. in *2015 12th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC)*. 2015. IEEE.
18. OKUTAN, A., S.J. YANG, and K. MCCONKY. *Predicting cyber attacks with bayesian networks using unconventional signals*. in *Proceedings of the 12th Annual Conference on Cyber and Information Security Research*. 2017. ACM.
19. PASSERI, P., *Hackmaggedon Information Security Timelines and Statistics*. 2017.
20. FARHADI, H., M. AMIRHAERI, and M. KHANSARI, *Alert correlation and prediction using data mining and HMM*. The ISC International Journal of Information Security, 2011. **3**(2): p. 77-101.

21. SENDI, A.S., et al., *Real time intrusion prediction based on optimized alerts with hidden Markov model*. Journal of networks, 2012. **7**(2): p. 311.

22. SHIN, S., et al., *Advanced probabilistic approach for network intrusion forecasting and detection*. Expert systems with applications, 2013. **40**(1): p. 315-322.

23. *Intrusion Detection Evaluation Dataset (CICIDS2017)*, U.o.N. Brunswick, Editor. 2017: https://www.unb.ca/cic/datasets/ids-2017.html.

24. *Snort - Network Intrusion Detection & Prevention System*. Available from: https://www.snort.org.

25. CALTAGIRONE, S., A. PENDERGAST, and C. BETZ, *The diamond model of intrusion analysis*. 2013, Center For Cyber Intelligence Analysis and Threat Research Hanover Md.

26. VELAZQUEZ, C., *Detecting and preventing attacks earlier in the kill chain*. SANS Institute Infosec Reading Room, 2015: p. 1-21.

27. QinetiQ, *Command & Control: Understanding, Denying, Detecting*. 2014.

28. *A View From Front Lines. 1st ed. MANDIANT A FireEye Company*. 2015; Available from: http://www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf.

29. AL-MOHANNADI, H., et al. *Cyber-attack modeling analysis techniques: An overview*. in *2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*. 2016. IEEE.

30. BOU-HARB, E., M. DEBBABI, and C. ASSI, *Cyber scanning: A Comprehensive Survey*. IEEE communications surveys & tutorials, 2013. **16**(3): p. 1496-1519.

31. ; Available from: https://www.mycert.org.my.

32. *SNORT Users Manual 2.9.13*. The Snort Project 2019; Available from: https://www.snort.org/documents/snort-users-manual.