8th International Conference on Computer and Knowledge Engineering (ICCKE 2018), October 25-26 2018, Ferdowsi University of Mashhad

Moving Target Defense against Advanced Persistent Threats for Cybersecurity Enhancement

Masoud Khosravi-Farmad, Ali Ahmadian Ramaki and Abbas Ghaemi Bafghi
Data and Communication Security Lab., Computer Engineering Department, Ferdowsi University of Mashhad, Mashhad, Iran
m.khosravi@mail.um.ac.ir, ali.ahmadianramaki@mail.um.ac.ir, ghaemib@um.ac.ir

Abstract - **One of the main security concerns of enterprise-level organizations which provide network-based services is combating with complex cybersecurity attacks like advanced persistent threats (APTs). The main features of these attacks are being multi-level, multi-step, long-term and persistent. Also they use an intrusion kill chain (IKC) model to proceed the attack steps and reach their goals on targets. Traditional security solutions like firewalls and intrusion detection and prevention systems (IDPSs) are not able to prevent APT attack strategies and block them. Recently, deception techniques are proposed to defend network assets against malicious activities during IKC progression. One of the most promising approaches against APT attacks is Moving Target Defense (MTD). MTD techniques can be applied to attack steps of any abstraction levels in a networked infrastructure (application, host, and network) dynamically for disruption of successful execution of any on the fly IKCs. In this paper, after presentation and discussion on common introduced IKCs, one of them is selected and is used for further analysis. Also, after proposing a new and comprehensive taxonomy of MTD techniques in different levels, a mapping analysis is conducted between IKC models and existing MTD techniques. Finally, the effect of MTD is evaluated during a case study (specifically IP Randomization). The experimental results show that the MTD techniques provide better means to defend against IKC-based intrusion activities.**

Keywords – cybersecurity; complex multi-step attack scenario; Advanced Persistent Threat (APT), Intrusion Kill Chain (IKC); Moving Target Defense (MTD).

I. Introduction

In today's modern world, regarding increasing the number of provided services using technologies such as cloud computing, virtualization platforms and service function chaining by internet service providers (ISPs), the computer networks has grown up. One of the main concerns of networks growth is occurrence of complex security related incidents due to increasing the size of the network, poor network management and less hardening of networks against cybersecurity attacks [1, 2]. Hence, the malicious attackers and adversaries have a good opportunity to attack the network to catch the sensitive data and/or sabotage the ICT systems.

One of the main challenges in large networks is combating with the new generation of cybersecurity attacks which are getting more and more complex and targeted e.g. advanced persistent threats (APTs) [3, 4]. Generally, in the APT attacks, the attackers follow a predefined attack phases which are known as Intrusion Kill Chain (IKC) [5]. Based on the drawn IKC model, the attackers use a set of intrusion activities to infiltrate the target network and obtain their final goals by compromising hosts. Although, the attackers use advanced attack vectors at side of attack surface, some promising approaches are proposed by the security research communities to combat and minimize the attacker's behaviors. One such approach is Moving Target Defense (MTD) [6, 7].

MTD techniques refer to a set of techniques that attempt to defend a system against APT attacks by increasing attacker's uncertainty of the system [6]. There have been several studies conducted on the effectiveness of applying various MTD techniques in increasing the security level of information systems. There are also several researches that present an overview of MTD techniques from different points of view. For instance, technical details of MTD techniques and their threat models alongside their weaknesses are described in [8, 9]. An overview on MTD technologies and strategies based on the research areas in the MTD field is presented in [7]. In [10], a three-layer model is proposed to evaluate and compare effectiveness of different MTDs. In [11], the authors have conducted some empirical experiments using various MTD approaches to evaluate their efficiency.

In this paper, common IKCs are presented and discussed and a taxonomy of MTD techniques in various levels is proposed. Moreover, a mapping analysis between IKC models and existing MTD techniques is conducted. Also, the effectiveness of applying MTD techniques is discussed and the feasibility study is examined using a case study.

The rest of the paper is organized as follows. In Section II, a detailed description of Intrusion Kill Chain (IKC) is provided. In Section III, the modern technology to mitigate APT attacks, namely, Moving Target Defense (MTD) is described. Section IV explains the proposed cybersecurity enhancement approach. In section V, the capabilities of the MTD techniques for preventing APT attacks is shown with a case study. Finally, Section VI concludes the paper and draws some future works.

II. Intrusion Kill Chain (IKC)

As mentioned before, one of the main security concerns of enterprise-level organizations is combating with complex APT attacks. These types of attacks have various destructive effects on the target network and its assets. These effects can cause confidential data manipulation or deletion, capturing keystroke, data exfiltration, accessing mails/files/passwords and even systems sabotage.

According to the literature, complex cybersecurity attacks as a subset of targeted attacks, have a set of unique characteristics which distinguishes them from the traditional types of attacks.

978-1-5386-9569-2/18/$31.00 ©2018 IEEE

The main special characteristics of the APT attacks are being multi-level, multi-step, long-term and persistent [2, 4, 12]. Multi-level is referred to the combined native of the attack which uses network, host and application levels to perform the intrusion. Multi-step indicates that the attack has a set of phases to complete the attack mission. Long-term says that the attack is happening over a long period of time. Also, persistence means that the attacker uses the compromised systems as a pivot for later intrusions.

Generally, malicious attackers and adversaries behind the complex APT attacks have access to sophisticated tools and different technologies to penetrate the targeted network. During the progression of the attack, they use different intrusion activities to achieve their goals. In other words, they carry-out a multi-step attack which is followed by a chain of individual actions [13]. In the area of intrusion detection, this chain of actions is called Intrusion Kill Chain (IKC) of an APT attack.

The Intrusion Kill Chain, also known as Cyber Kill Chain, is a methodology based on a set of intrusion activities which implies the different steps/stages of an APT attack scenario. By using the IKC, it is possible to track the attacker's behaviors during the attack life cycle. Thus, one of the main usage of the IKC is attack modeling in defensive technologies e.g. Intrusion Detection Systems (IDSs) to detect security incidents. So, the provided knowledge from the IKC modeling of an incident can help security teams to analyze, tackle and mitigate attacks by using modern countermeasures like MTD solutions.

To the best of our knowledge, based on a systematic literature review, there are some IKC models proposed in the area of intrusion detection. The details of the existing IKC models are presented in Table I. As shown in Table I, one of the key features of the IKC models is the IKC types. IKC type indicates the nature of attack life cycle which is categorized in two types, namely, Linear and Circular. In the linear models (Fig. 1 (A)) like ZScaler [15], the event sequences of an attack are explained in a linear direction. It means that when the attackers achieve their goals, they leave targeted network. In contrast, in the circular models (Fig. 1 (B)) like Lockheed Martin [13], the steps of the IKC is repeated by the attacker for a long time while the connections are maintained with the external command and control (C2) servers. Since, in a real APT attack scenario, the attacker maintains the accesses on the compromised nodes and repeats the attack stages continuously, the circular model is better than the linear one to simulate the adversaries' behaviors.

TABLE I. THE EXISTING INTRUSION KILL CHAIN MODELS

No.	***IKC Name***	***Type of IKC***	***Year***	***Reference***
1	Bryant	Circular	2017	[5]
2	Dell	Circular	2016	[16]
3	ZScaler	Circular	2015	[15]
4	Pandey	Linear	2014	[14]
5	Mandiant	Linear	2013	[17]
6	Symantec	Circular	2012	[18]
7	Lockheed Martin	Linear	2011	[13]

After identification of the existing IKC models, it is time to select a basic model and do the further analysis on the basis of the selected model. To this aim, the mentioned IKC models in Table I are compared with each other. The results of the comparison are shown in Table II. According to the Table II, the most important metrics are Number of Steps (indicates the number of attack steps in the IKC model), Dedicated Levels (based on the multi-level nature of the APT attacks), Main Focus (to determine the main intrusion activity of the model) and Main Usages (to find the main security incidents of the Model).

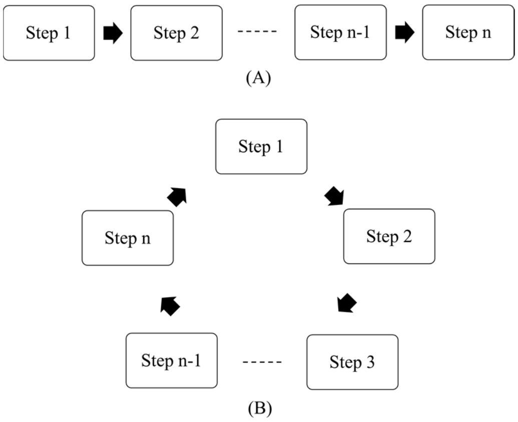

FIGURE I. TYPES OF IKC MODELS, (A) LINEAR AND (B) CIRCULAR

Based on the Table II, all the existing IKC models use the vulnerabilities of the three aforementioned levels to break into the network by using various types of attack methods. For example, the main attack methods in network level are enumeration, scanning, social engineering and spear phishing. The methods of the host level contain vulnerability exploitation, malicious code execution, rootkit and backdoor installation and privilege escalation. Also, the attack methods against the application level can be named as accessing mail, files and passwords, violation against data (manipulation/deletion) and also SQL injection attacks.

TABLE II. COMPARISON BETWEEN THE EXISTING IKC MODELS

No.	***#of Steps***	***Dedicated Levels***	***Main Focuses***	***Main Usages***
1	7	Network, Host and Application	Lateral Movement	Exfiltration, DoS and Destruction
2	8	Network, Host and Application	Initial Breach	Exfiltration
3	4	Network, Host and Application	Lateral Movement	Exfiltration and Destruction
4	10	Network, Host and Application	Internal Reconnaissance	Exfiltration
5	8	Network, Host and Application	Internal Reconnaissance	Exfiltration and Destruction
6	4	Network, Host and Application	Initial Breach	Exfiltration and Destruction
7	7	Network, Host and Application	Initial Breach	Exfiltration and Destruction

After comparison analysis, to study the mapping analysis of MTD solutions and IKC models, it is required to select a suitable model which is appropriate for further scrutiny. Hence, in order to further analysis of the attack steps of a selected IKC model (steps mapping with the MTD solutions), the Bryant kill chain model is selected due to being a circular model, covering the intrusion activities in all three levels (application, host and network), newer than the other models and also containing the internal and external reconnaissance activities and also usable for a wide range of use cases.

Bryant model is a new IKC model which is proposed by Bryant and Saiedian in 2017 [5]. This model has been made using some modifications to previous models e.g. Lockheed Martin and Mandiant models [5, 13-18] which makes it a suitable choice for data-driven analyzes in security information and event management (SIEM), security operation center (SOC) and also threat modeling methods (TMM). The main steps of the Bryant kill chain and the related levels of them is depicted in Fig. 2. The color range from green to red shows that the more the attack progresses, the possible damages caused by the attack increases. Thus, when the attack is in its early stages, deceiving the attackers and hardening the network against their intrusion activities is more important and is more beneficial.

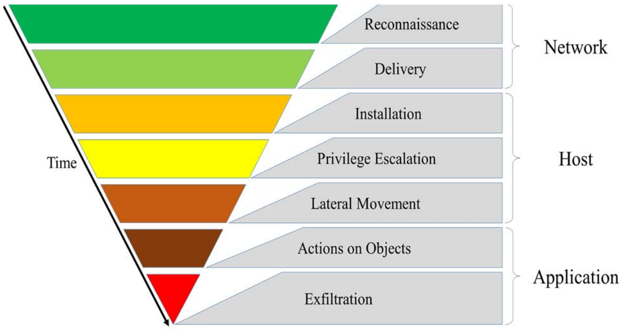

FIGURE 2. BRYANT KILL CHAIN STEPS AND THE RELATED LEVELS

As shown in Fig. 2, the Bryant IKC consists of seven steps which are described as follows:

1. Reconnaissance: In this step, the attackers gather information about the target. The main objective of this step is gaining knowledge about the victim and finding the effective methods and technologies to intrude the network.
2. Delivery: In this step, the attackers try to deliver a prepared attack payload to the network by using the established connections between a victim or a collection of victims.
3. Installation: In this step, the main objective of the attackers is installation of attack payload/malwares on the infected systems. This step is necessary for a persistent accessing in further intrusion activities.
4. Privilege Escalation: In this step, the objective of attackers is to escalate their privileges on the victims which helps them to move the target in order to find valuable information.
5. Lateral Movement: The main objective of this step is to differentiate between the reconnaissance activity from the external and internal network. Internal reconnaissance is used for moving laterally within the compromised organization.
6. Actions on Objects: By using this step, the adversaries achieve the attack’s goal by performing several small steps inside the target network which can take months.
7. Exfiltration: In this step, after a successful execution of attack steps on the final objects, the attackers attempt to exfiltrate sensitive data form the target network by using suitable communication and control (C&C) nodes.

After explanation of the IKC models and especially Bryant IKC model, the MTD and it’s relations to the steps of IKC for mitigating and preventing APT attacks is described in the following section.

III. MOVING TARGET DEFENSE (MTD)

Moving Target Defense (MTD) is a series of proactive defensive security techniques which continuously changes the attack surface of the protected systems to reduce the chance of them being compromised [6]. Attack surface is defined as available set of ways an attacker can use to enter the system and inflict damage [19]. MTD techniques do not aim at removing vulnerabilities but, instead, they focus on disrupting attacker’s abilities to perform reconnaissance and vulnerability exploitation.

Generally, MTD techniques fall into three levels namely application-based, host-based, and network-based which are described as follows, respectively.

- **Application-based MTD** work by manipulating applications code dynamically in order to protect applications against analysis, thereby limiting vulnerability exposure to attackers. Dynamic runtime environment techniques fall into this category. For example, Address Space Layout Randomization (ASLR) techniques dynamically change the memory layout of a process to stop attackers from easily manipulating known absolute and relative addresses [20] and Instruction Set Randomization (ISR) [21] techniques dynamically change the underlying instruction set of programs to stop attackers from injecting and executing valid codes.
- **Host-based MTD** divide into software-based and hardware-based techniques. These techniques may change different properties of hosts and platforms such as OS version, OS instance, or CPU architecture in order to increase the uncertainty in the attacker side [8]. Host-based MTD techniques are often implemented using virtualization.
- **Network-based MTD** change network properties dynamically to disrupt attacks by confusing attackers. Examples of these techniques are IP address and/or port hopping [22], routing path randomization [23] and proxy-location randomization [24].

A detailed classification from the viewpoint of techniques for each of the aforementioned levels are Shuffle-based, Diversity-based and Redundancy-based techniques.

- **Shuffle-based techniques** reorder system configuration dynamically in various system layers [22, 25], e.g. IP/port hopping, application/VM migrations, data/address/instruction set randomizations and topology rearrangements.
- **Diversity-based techniques** provide functionally equivalent variants of a system with different implementations [26]. These techniques are mainly divided into Software-based Diversification, Runtime-based Diversification, Communication-based Diversification and Dynamic Platform Techniques [10].
    - Software-based Diversification is achieved by directly manipulating the software or making compilers to produce diversification.
    - Runtime-based Diversification techniques try to introduce diversification in runtime environments. Address Space Layout Randomization (ASLR) techniques fall into this category.
    - Communication-based Diversification techniques mostly try to hide communication protocols from outsiders to protect the system against network related attacks.
    - Dynamic Platform Techniques (DTP) periodically change the underlying platform properties to stop the attackers from penetrating the system. Virtual machine rotation and multiple variants execution techniques are two widely used techniques that fall into this category.
- **Redundancy-based techniques** provide multiple replicas of a service or a system component with the same function in topology or application layers [27].

After detailed explanation of the IKC and MTD concepts in Section II and Section III respectively, the mapping analysis between IKC steps and the MTD solutions in different levels are discussed in the next section.

IV. Proposed Cybersecurity Enhancement Approach

As mentioned in Section II, the network intruders and adversaries typically use the IKC steps to penetrate the target network and accomplish their mission. Based on our analysis, we have selected the seven steps of the Bryant kill chain. Also, the capabilities of the MTD techniques for preventing the complex cybersecurity attacks are described in Section III. In this section, the relationships between each step of the IKC and the existing MTD techniques are explained.

Table III lists the IKC steps in each of the network, host and application domains with attack methods applicable within them. It also includes some of the most common MTD techniques to counter attack methods of each IKC step.

TABLE III. IKC and MTD Mapping Analysis

Domain	***IKC Step***	***Attack Method***	***MTD Techniques***
Network	Reconnaissance	Probing	IP Randomization, Port Hopping, Topology Rearrangement, OS Randomization, Routing Path Randomization, Proxy-location Randomization
		Fingerprinting	
		Social Engineering	
		Vulnerability Scanning	
	Delivery	Host Access	IP Randomization, Port Hopping, Topology Rearrangement, OS Randomization, Routing Path Randomization, Proxy-location Randomization
		Network Delivery	
Host	Installation	Configuration Changes	Address Space Layout Randomization (ASLR), Instruction Set Randomization (ISR), Executable Space Protection, OS Randomization, System Call Randomization,
		Malicious Code Execution	
		Backdoor and Rootkit Installation	
	Privilege Escalation	Privilege Escalation	Address Space Layout Randomization (ASLR), Privilege Separation, Compiler Access Restriction
		Privilege Use	
	Lateral Movement	Information Gathering	IP Randomization, Port Hopping, Topology Rearrangement, OS Randomization, Routing Path Randomization, Proxy-location Randomization
		Internal Reconnaissance	
		Command Execution	
Application	Actions on Objects	Software Modification	Address Space Layout Randomization (ASLR), Instruction Set Randomization (ISR)
		Data Manipulation/Deletion	
		Obfuscation	
		Removing Intrusion Logs	
	Exfiltration	Accessing Mail, File and Passwords	Access Control, Encryption, Distributed Storage, Watermarking, SQL
		Data Theft	

Generally, during a targeted APT attack, attackers move through three main domains namely Network, Host and Application. The attackers use one or more steps of the IKC in each of the mentioned domains. For example, in the network domain, the common IKC steps are Reconnaissance and Delivery. There are several attack methods available to the attackers in each of the IKC steps. For example, attack methods in Reconnaissance step are Probing, Fingerprinting, Social Engineering and Vulnerability Scanning. Some of the common MTD techniques to counter these attack methods are IP randomization, port hopping, topology rearrangement, OS randomization, routing path randomization and proxy-location randomization.

As mentioned before, APT attacks have a set of special characteristics such as multi-level, multi-step, long-term and persistent. Using MTD techniques in Table III, the network coverage is provided against APT attacks by nullifying the mentioned APT attack features. Regarding multi-level feature, applying different MTD techniques in various levels help to defend the network. Also, applying different MTD techniques during the steps of attacks guaranty that the extracted results by the attackers from the victim nodes in a step cannot be used for further steps. Indeed, long-term native of the APT allows MTD techniques e.g. IP randomization and port hopping to change the attack surface over time. Finally, some MTD techniques overcome the persistent native of the APTs to loss the obtained accesses to the compromised machines.

V. Feasibility Study and Discussion

In this section, the effectiveness of the MTD techniques to combat complex APT attacks is presented during a case study. The objective of the case study to show the power of a specified MTD technique, IP address randomization, which is a good choice to prevent the outside network for locating and targeting real hosts. Since in all of the APT attack scenarios, attackers use different methods to identify the target network during the reconnaissance step, the IP address randomization is selected and evaluated. Based on this technique, the IP addresses of the network hosts is randomly refreshed and reassigned over the time.

In the area of intrusion detection systems, one of the famous intrusion detection datasets is constructed by the ISCX in the University of New Brunswick in 2012 [28]. The ISCX dataset has a multi-step APT attack scenario based on the Bryant IKC model which is known as infiltration attack. Based on this attack scenario, the attacker intrudes a network and then walks around within the internal network. After the initial breach by using a malicious attachment, the attacker harvests valuable credential data and accesses sensitive files after a successful SQL injection attack. The attack scenario is shown in Fig. 3.

According to the Fig. 3, the main steps of this attack scenario regarding to the Bryant IKC model are as follows:

1. Reconnaissance: The attacker gathers information about the target network form outside by using a social engineering attack. In this step, a windows host with IP address 192.168.1.105 is identified which contains a vulnerability on the Acrobat Reader 8 application.

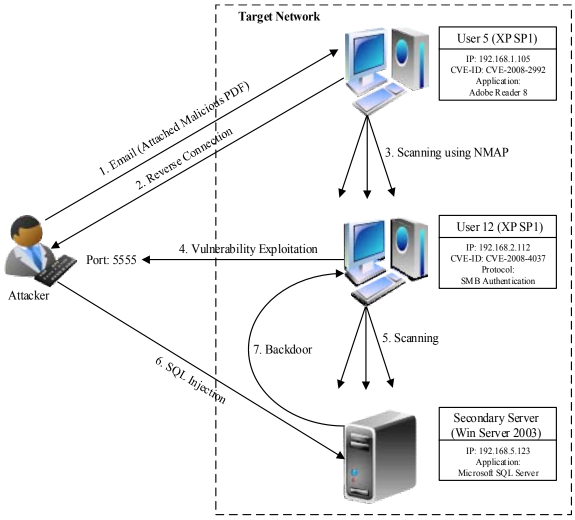

FIGURE 3. INFILTRATION ATTACK SCENARIO IN ISCX DATASET [29]

2. Delivery: In this step, the attacker tries to send an email with a malicious PDF payload to deliver it to the target node of the subnet 192.168.1.0/24 (steps 1 and 2 in Fig. 3).

3. Installation: In this step, the attacker establishes a persistent connection to the compromised node after installation of the malicious payload on it and obtains a reverse connection for accomplishing later attack steps.

4. Privilege Escalation: In this step, the attacker escalates his/her privilege for running privileged programs like sniffing and scanning attack tools e.g. NMAP (step 3 in Fig. 3).

5. Lateral Movement: By using the NMAP security scanner, the attacker scans the other subnet of the target network to obtain a server with noteworthy information. In this step, after scanning subnets 2/24 and 5/24 and exploitation of their vulnerable hosts, the attacker reaches a windows-based web server including vulnerable SQL server (steps 4 and 5 in Fig. 3).

6. Actions on Objects: By using vulnerability in the SQL server, the attacker starts to perform a SQL injection attack for accessing the sensitive files in it and creates a backdoor for preserving accesses (steps 6 and 7 in Fig. 3).

7. Exfiltration: In this step, after a successful SQL injection attack on the final compromised node with IP address 192.168.5.123, the attacker attempts to theft SQL database files which contains sensitive data.

The objective of this experiment is to disrupt the Reconnaissance and Delivery steps of the IKC model by choosing IP randomization MTD technique in the network domain. With IP randomization technique implemented on the network (using IP Switcher tool [30]), the network would change its IP address frequently and synchronize new IP addresses with authorized users only. Therefore, it causes delays in the attacks, since the attacker should periodically search for the targeted host new IP address.

As the result, by implementing IP address randomization technique, the attacks are disrupted by confusing attackers. Assume that prevention ability of each MTD technique in each of the IKC steps is α percent successful, the probability of successful attack will be (1-α). Hence, according to the seven steps of the Bryant IKC model, the total probability of successful attack will be decreased to $(1-\alpha)^7$ which significantly enhances the total security level of the network.

VI. Conclusion and Future Works

Nowadays, complex cybersecurity attacks such as APTs are becoming a great concern for network security administrators. Due to the nature of these attacks, they cannot be prevented by traditional security solutions. Hence, deception techniques such as MTD techniques are proposed by security researchers which are suitable for combating against these modern attacks. In this paper, we first present and discuss common IKCs and also propose a taxonomy of MTD techniques in various levels. After that, we conduct a mapping analysis between IKC models and existing MTD techniques. Finally, the effectiveness of applying MTD techniques is discussed and the feasibility study is examined using a case study. In future, we try to assess the security level of MTD-based systems using graphical security models.

References

[1] Ramaki, A. A., Amini, M., & Atani, R. E. (2015). RTECA: Real time episode correlation algorithm for multi-step attack scenarios detection. computers & security, 49, 206-219.

[2] Liu, L., De Vel, O., Han, Q. L., Zhang, J., & Xiang, Y. (2018). Detecting and Preventing Cyber Insider Threats: A Survey. IEEE Communications Surveys & Tutorials, 20(2), 1397-1417.

[3] Ramaki, A. A., Rasoolzadegan, A., & Bafghi, A. G. (2018). A systematic mapping study on intrusion alert analysis in intrusion detection systems. ACM Computing Surveys (CSUR), 51(3), 55.

[4] Ramaki, A. A., Khosravi-Farmad, M., & Bafghi, A. G. (2015, September). Real time alert correlation and prediction using bayesian networks. In Information Security and Cryptology (ISCISC), 2015 12th International Iranian Society of Cryptology Conference on (pp. 98-103). IEEE.

[5] Bryant, B. D., & Saiedian, H. (2017). A novel kill-chain framework for remote security log analysis with SIEM software. computers & security, 67, 198-210.

[6] Carvalho, M., & Ford, R. (2014). Moving-target defenses for computer networks. IEEE Security & Privacy, 12(2), 73-76.

[7] Cai, G. L., Wang, B. S., Hu, W., & Wang, T. Z. (2016). Moving target defense: state of the art and characteristics. Frontiers of Information Technology & Electronic Engineering, 17(11), 1122-1153.

[8] Okhravi, H., Rabe, M. A., Mayberry, T. J., Leonard, W. G., Hobson, T. R., Bigelow, D., & Streilein, W. W. (2013). Survey of cyber moving target techniques (No. MIT/LL-TR-1166). Massachusetts Inst. of Tech., Lexington Lincoln Lab.

[9] Okhravi, H., Hobson, T., Bigelow, D., & Streilein, W. (2014). Finding focus in the blur of moving-target techniques. IEEE Security & Privacy, 12(2), 16-26.

[10] Xu, J., Guo, P., Zhao, M., Erbacher, R. F., Zhu, M., & Liu, P. (2014, November). Comparing different moving target defense techniques. In Proceedings of the First ACM Workshop on Moving Target Defense (pp. 97-107). ACM.

[11] Van Leeuwen, B., Stout, W., & Urias, V. (2016, October). MTD assessment framework with cyber attack modeling. In Security Technology (ICCST), 2016 IEEE International Carnahan Conference on (pp. 1-8). IEEE.

[12] Sood, A. K., & Enbody, R. J. (2013). Targeted cyberattacks: a superset of advanced persistent threats. IEEE security & privacy, 11(1), 54-61.

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

[14] Pandey, S. K., & Mehtre, B. M. (2014, April). A Lifecycle Based Approach for Malware Analysis. In Communication Systems and Network Technologies (CSNT), 2014 Fourth International Conference on (pp. 767-771). IEEE.

[15] Lima, A. J. C. (2015). Advanced persistent threats (Doctoral dissertation).

[16] Dell SecureWorks. (2015). Breaking the kill chain- knowing, detecting, disrupting and eradicating the advanced threat.

[17] McWhorter, D. (2013). APT1: Exposing one of China's cyber espionage units. Mandiant. Com, 18.

[18] Symantec. Advanced persistent threats: A symantec perspective. (2012), Technical Report.

[19] Manadhata, P. K., & Wing, J. M. (2011). An attack surface metric. IEEE Transactions on Software Engineering, 37(3), 371-386.

[20] Shacham, H., Page, M., Pfaff, B., Goh, E. J., Modadugu, N., & Boneh, D. (2004, October). On the effectiveness of address-space randomization. In Proceedings of the 11th ACM conference on Computer and communications security (pp. 298-307). ACM.

[21] Barrantes, E. G., Ackley, D. H., Palmer, T. S., Stefanovic, D., & Zovi, D. D. (2003, October). Randomized instruction set emulation to disrupt binary code injection attacks. In Proceedings of the 10th ACM conference on Computer and communications security (pp. 281-289). ACM.

[22] Chavez, A. R., Stout, W. M., & Peisert, S. (2015, September). Techniques for the dynamic randomization of network attributes. In Security Technology (ICCST), 2015 International Carnahan Conference on (pp. 1-6). IEEE.

[23] E. Al-Shaer and Q. D. J. Jafarian (2012, June). On the Random Route Mutation Moving Target Defense, in National Symposium on Moving Target Research.

[24] Jia, Q., Sun, K., & Stavrou, A. (2013, July). Motag: Moving target defense against internet denial of service attacks. In Computer Communications and Networks (ICCCN), 2013 22nd International Conference on (pp. 1-9). IEEE.

[25] Jafarian, J. H., Al-Shaer, E., & Duan, Q. (2012, August). Openflow random host mutation: transparent moving target defense using software defined networking. In Proceedings of the first workshop on Hot topics in software defined networks (pp. 127-132). ACM.

[26] Newell, A., Obenshain, D., Tantillo, T., Nita-Rotaru, C., & Amir, Y. (2015). Increasing network resiliency by optimally assigning diverse variants to routing nodes. IEEE Transactions on Dependable and Secure Computing, 12(6), 602-614.

[27] Kirrmann, H., & Dzung, D. (2006, June). Selecting a standard redundancy method for highly available industrial networks. In Factory Communication Systems, 2006 IEEE International Workshop on (pp. 386-390). IEEE.

[28] Shiravi, A., Shiravi, H., Tavallaee, M., & Ghorbani, A. A. (2012). Toward developing a systematic approach to generate benchmark datasets for intrusion detection. computers & security, 31(3), 357-374.

[29] Ahmadian Ramaki, A., & Rasoolzadegan, A. (2016). Causal knowledge analysis for detecting and modeling multi-step attacks. Security and Communication Networks, 9(18), 6042-6065.

[30] Free IP Switcher V3.0, (Available onlie: https://filehippo.com/download_free_ip_switcher/).