International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878,Volume-8, Issue-1C, May 2019

Shuffle-Selective-Search Process for Mitigation of APTs with IKC

Abdul Khadar, Shrishail Math, H. Srinivasa Murthy

Abstract: ***Data forensics is a process of recognizing, protecting, recovering, evaluating, and presenting features of magisterial digital information. This data could lead to sensitive information of an organization or a person. The APTs are intended to invade the system or environment of this data and try to be in the environment till the successful theft. Advanced Persistent Threats (APTs) follow the Intrusion Kill Chain (IKC) to be successful. This paper proposes a prospecting "shuffle-selective-search" dissection to be inducted in phases of IKC to identify the intrusion-point in the system. Where- in which an effort is made to identify the APT attack as it follows the IKC, by the Shuffle-Selective-Search dissection when there is an intrusion at the intrusion-point within the forensic data repository.***

Key-words: shuffle-selective-search, APTs, IKC, intrusion-point

I.INTRODUCTION

Forensic data is most sensitive and highly valuable data of an organization or of a person, breaching of which may cause financial or moral or societal or security disservice. An organization's forensic data may possess organization business or management policies, security issues, employees personal and professional details etc., An individual's forensic data may be the personal details, images, videos or legal documents. A government forensic data could be the national defense details, security matters, political scenarios and situations etc., There could be criminal forensic data, health forensic data, any data for that matter which has high value and importance for the concerned authority. This data has to be safeguarded by the owner from the invaders so as to avoid data breach.Advanced Persistent Threats (APTs) [3][1], as there is highly sensitive and valuable data there are always illegal and invading users to get unauthorized access and control of it. The surreptitious computer network attack by an unauthorized faction of people or an individual who take over the access and control of the system and pro-exist in the system environment for further and complete access and success for prolonged duration without any waft to the firewalls or intrusion detection system established for the system security are the Advanced Persistent Threats.APTs have 3 main phases of execution in broad sense, they are Infiltration, Expansion and Extraction [5] where the invader tries to get into the system environment through some possible media like mails, memory cards, mobile apps or some entry point so that the Trojan can be embedded within the system.

Revised Manuscript Received on May 21, 2019

Abdul Khadar A, Ph.DScholor, Assistant Professor, Department of ISE, SJCIT, Chickballapur, Karnataka, India.

Dr.Shrishail Math, Prof. Department of ECE, SKIT, Bangalore, Karnataka,

H Srinivasa Murthy, Associate Professor Department of Computer Science and Engineering, SJCIT, Chickballapur, Karnataka, India.

Then the Trojan tries to gain access and control upon the system where it is not filamentous to the authority. Later in the process it extracts and transfers theforensic data to the external system though the backdoor and be persistent in the system.For example the APT 10 group, also known as Red Apollo and MenuPass [10], according to the indictment unsealed is believed to focus on espionage, including gathering military intelligence. It gains access to corporate and government systems via malware attached to email. The group has allegedly carried out attacks in at least 15 countries, including the U.S., Japan, the U.K., France, India and Australia during December 2018According to Lockheed Martin Corporation model, Intrusion Kill Chain [9] is an unavoidable stages of action that an intruder carries out in order to invade the target. The inception is from Information-Collection about the target that encompass choosing the target, knowing the facts about the target, like collecting mail ids, web sites or linking URLs, the in and out of the methods and ways technically the target safeguard his information, the business and financial circle of the target and the modes in which the target does his financial and personal transactions.The step immediate to follow is weaponization that involves embedding of malevolent code into the non-doubtful carriers of this code like mails, files, memory cards to reach the target. The stage next is executing this plan to reach the target environment. This step will be done carefully with utmost caution so as to keep the target unaware of the incubation into the computer network of the target.As the target environment is reached by the Trojan the very next stage of the IKC is to get into susceptibility of the target environment to execute the malevolent code so the stage is known as exploitation that is finding the most unsuspected or un-doubtful area inside the target environment.The stage next is to install the malevolent code into incubated environment with only intension to maintain persistency and find the most unsuspected method of being executed which may involve the distributed denial of service (DDoS) [11] attack by the invader in the target environment usually Remote Access Trojan's (RAT) are used here.Gaining the command and control at the point of attack or remotely is the next stage. Here is where the invader tries to establish non-fishy communication channel with target environment. And persistently do so till the successful end of mission. The last stage of IKC is the actual action which may involve the extraction of needed forensic data and information from the target environment and transferring it to the external unauthorized location.

Retrieval Number: A10170581C19/19©BEIESP

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

This whole process will be conducted over a long period of time, stage by stage being unsuspected and successful.

II. RELATED WORK

Malicious Data Leak Prevention and Purposeful Evasion Attacks: An Approach to Advanced Persistent Threat (APT) Management" [1] by Tarique Mustafa presents a three dimensional parallel model to defend the sophisticated APTs.The method is split into gaining insight into the anatomy of APTs that cause MDL, involves understanding the taxonomy of Evasion Attacks that these APTs can launch to cause failure of Egress Control and provide a DLP paradigm that can effectively stop MDL caused by APTs."A Graph Analytic Metric for Mitigating Advanced Persistent Threat" by John R. Johnson and Emilie A. Hoganthough suggests there is scope for future work, it proposes a γ_v– metric of a vertex v, in graph H, is defined as the number of vertices of H on a path concluding at v from u, as $\gamma_v = \Sigma$ p (u, v) where u $\in$ H. By these primitives, it is easy to define the reachability graph as an oriented sub graph of the fully connected graph based upon the mechanics of the authorization aspects of network security and the salient characteristics of a particular vulnerability. It is proposed that this metric used to quantify the risk of exposure to potential cyber security threats such as Pass-The-Hash.It is also proposed that in reality it is possible to calculate the γ_v metric at the authorized stage of computer network security for providing the network manager the right to configure his network to reduce or mitigate the problem due to exposure to the APTs."Towards a Framework to Detect Multi-Stage Advanced Persistent Threats Attacks" by Parth Bhatt, Edgar Toshiro Yano and Dr. Per M. Gustavsson [3] suggests a comprehensive framework to control the intrusion with the help of Hadoop's trending technologies like Pig, Hive etc., The use of the IKC attack model allows a better tuning of the configuration of security controls and it can be used as a hypothesis model to improve the correlation of logs and thereby facilitate the identification of ongoingattacks."A Game Model for Predicting the Attack Path of APT" work by Xupeng Fang, LidongZhai, ZhaopengJia, WenyanBai [4] describe the OAPG model that is applied to predict the optimal attack path of APT in Internet of things. Base on the new calculation method of reward, it computes the optimal attack path for attacker and best-response strategies for the defender. This work also proposes a method to apply this model to large-scale network. Using the game theory view with help of Nash equilibrium it computes the optimal attack path and the optimal confrontation for the defender."Multi-Agent System for APT Detection" work by WimMees, ThibaultDebatty [5] propose a new system that combines multiples approaches using advanced aggregation techniques to achieve a better detection performance. It also test the system on real data from a small corporate network, and show that the system is able to attain a high probability of detection to probability of false alarm ratio."Incorporating the Human Element in Anticipatory and Dynamic Cyber Defense" work by AunshulRege [6] suggests that from the information from ICS-CERT there is an emergency need for some monitoring and control of APTS which could be ease to do with IKC knowledge. The work offers recommendations for further research and the relevance of multidisciplinary collaboration."Moving Target Defense against Advanced Persistent Threats for Cybersecurity Enhancement" a work by MasoudKhosravi-Farmad, Ali AhmadianRamaki and Abbas GhaemiBafghi [7]. According to this research one can choose one of the IKC stages for analysis of the attack by the invader and a taxonomy of MTD methods is suggested at various levels and a comparison is done between the IKC models and the MTD methods. The results suggests that the MTD is better.

III. SHUFFLE-SELECTIVE-SEARCH (SSS) PROCESS TO MITIGATE APTS WITH IKC

The Shuffle-Selective-Search [8] dissection is a process of identifying the intrusion of the invaders into the forensic data environment through IKC method.As the APTs are conducted over the forensic data repeatedly and continuously for a prolonged period of time to gain the access and control over the intrusion-point environment the SSS dissection suits well to mitigate the APTs that follow IKC to succeed the attack. It works on the pair of computer networks of the organization or forensic data environment where each computer of the network could be identified by a unique number like IP address.These IP addresses need to be taken as an array of elements in an order.

A. SSS Process

Step 1: Initialize the size of the array in terms of power of 2 i.e. size=2^n

Step 2: Assign 2^n elements to array in ascending order from 1 to 2^n

Step 3: Display the 2^n elements of the array as equally divided buckets i.e., $2^n/2$ elements as bucket 'A' & remaining $2^n/2$ elements as bucket 'B'

Step 4: Assume an element in the array i.e., Key and select the bucket the key belongs to i.e., either bucket 'A' or bucket 'B'

Step 5: Shuffle the elements of both the buckets with bucket 'A' elements followed by bucket 'B' elements.

Step 6: Repeat through Step 3, n-1 times.

Step 7: The assumed Key is present at if (n<=5) then position = (square of odd number previous to n)+1 else if (n>=6) then position = $2^n/2$-22(if key is in bucket 'A') or 2^n-22 (if key is in bucket 'B')

This dissection has to be carried out manually by the network administrator by selecting one of the networks of the pair of networks, under threat.

B. SSS Working

The SSS [8] process starts with following assumption 1) the minimum size of the array is 16 i.e., 2^4=16 where n=4, andif more than 16 then the size should be multiple of 16 2) the elements are in ascending order from 1 to 2^n i.e., from 1 to 16 for n=4. 3) the user has to assume the key and keep providing the bucket name ('A' or 'B') for n-1 number of shuffles.With these assumptions if the IPs of the network or the forensic data environment computers are assigned to an array and divided into 2 equally sized buckets. If the

Retrieval Number: A10170581C19/19©BEIESP

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

size of the network is 16 systems where n=4 and 2^n = 16 after n-1 (i.e., 3) shuffles the key will be fixed at position = 1^2+1 ((square of odd number previous to n) +1) if after last shuffle key is found in bucket 'A' or at position = 3^2+1 ((square of odd number previous to n) +1) if after last shuffle key is found in bucket 'B'.And if the size of the network is more than 2^4 i.e., n>=5 then the key assumed will be fixed after n-1 shuffles at position = 2^n/2-22 if after last shuffle key is found in bucket 'A' or at position = 2^n/-22 if after last shuffle key is found in bucket 'B'.Here the Key is the IP address of the network's computer which the invader is trying intrude and remain hidden inside the network persistently until the attack is successful.The algorithm needs the computer network administrator's interaction so as to select which network out of a pair of networks is doing fishy action or misbehaving but cannot identify the exact IP where the intruder is hidden and trying to invade the network.By this SSS process the network administrator can identify the exact IP where the computer misbehavior is happening and can locate the exact IP addressed computer after n-1 shuffles of the IPs within the pair of the networks. Since the APTs are the persistent attacks that last for long period of time for the successful attack this SSS algorithm if followed and implemented into the IKC process followed by the APT attackers any or all the steps after weaponization could lead to detect the intruder and the computer in the network where the intrusion is happening.

C. Result and Analysis

With the experiments done on the SSS process with data size starting from 16 bits and multiples of 16 is that it works well with identification of intrusion point in the forensic data environment and the intrusion-point could be fixed.

Table1. Result and analysis

Data Range	Data Size		No of Shuffles	Key position	
				Bucket 'A='	Bucket 'B'
n<6	n=4	$2^n=2^4=16$	n-1=3	$1^2+1=2$	$3^2+1=10$
	n=5	$2^n=2^5=32$	n-1=4	$3^2+1=10$	$5^2+1=26$
n>=6	n=6	$2^n=2^6=64$	n-1=5	$2^6/2-22=10$	$2^6-22=42$
	n=7	$2^n=2^7=128$	n-1=6	$2^7/2-22=42$	$2^7-22=106$

with least efforts if implemented at the IKC stages.

The above analysis of the result could be plotted as graph as shown in following Figures. The graph in Figure1 depicts the 4 different scenarios of different size of network which is under threat and if after the n^{th} shuffle the bucket 'A' is found to have the intrusion-point then the point of intrusion is given by the 'Key Position' in each case.

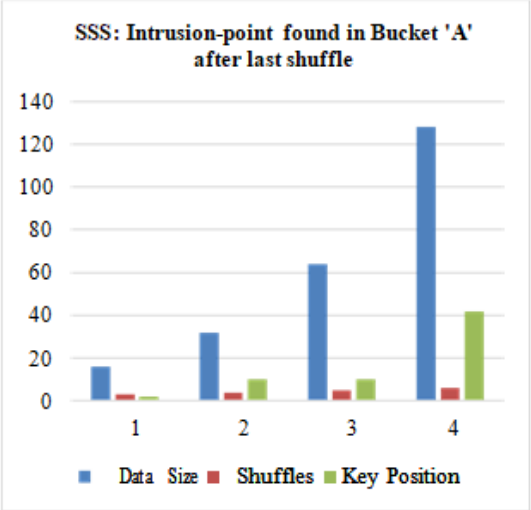

Fig1. Graph of intrusion-point in Bucket'A'afterlastshuffle.

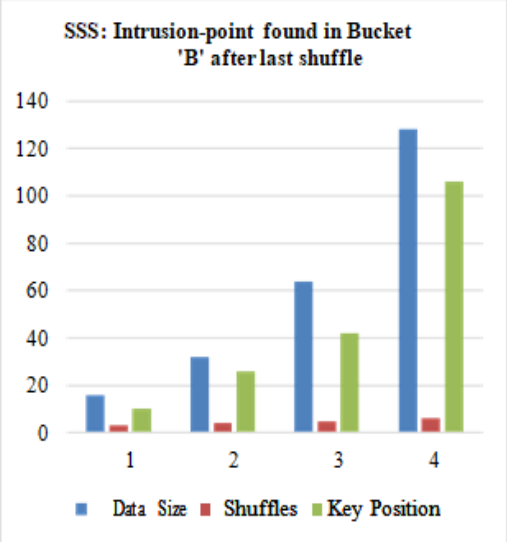

Fig2. Graph of intrusion-point in Bucket'B'afterlastshuffle.

The above graph in Figure2 depicts the 4 different scenarios of different size of network which is under threat and if after the n^{th} shuffle the bucket 'B' is found to havethe intrusion-point then the point of intrusion is given by the 'Key Position' in each case.

The plot in figure3 shows the line graph of the size of the network, the number of shuffles for each size network and the intrusion-point in each case if the it is found in the bucket 'A' or in bucket 'B'. The analysis shows that the number of shuffles increases by one for every doubling of the size of the network which is a good sign of the SSS dissection that does not stalls the intrusion detection for the doubled network size.

Retrieval Number: A10170581C19/19©BEIESP

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

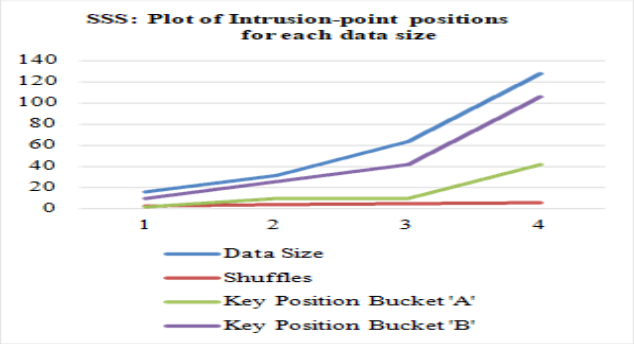

Fig3. Plot of intrusion-point positions for each data size

IV. CONCLUSION AND FUTURE ENHANCEMENTS

As the Shuffle-Selective Search process is suitable for the APTs that last for long period of time it is not restricted by time or space complexities. As the implementation of this process need the actual Data Forensic environment and IDS (intrusion detection system) the working of this process is simulated with help of arrays of elements of natural numbers from 1 to 2^n as contents of the array.There is scope for enhancement over this SSS process so as to scale the number of computers in the pair of the network to actual numbers. The process as in fact verified for the result with number of computer systems in the pair of networks from 16 (2^4) till 128 (2^7) and the higher multiple of 16 number of computers in the network pair is yet to be verified and analyzed.

REFERENCES

1. Malicious Data Leak Prevention and Purposeful Evasion Attacks: An Approach to advanced Persistent Threat (APT) Management, Tarique Mustafa, Founder & Chief Executive Officer / Chief Technology Officer, nexTier Networks, Inc.2953, Bunker Hill Lane, Ste: 400, Santa Clara, CA-95054,USA
2. A Graph Analytic Metric for Mitigating Advanced Persistent Threat John R. Johnson and Emilie A. Hogan
3. Towards a Framework to Detect Multi-Stage Advanced Persistent Threats Attacks, Parth Bhatt, Edgar Toshiro Yano, Dr. Per M. Gustavsson
4. A Game Model for Predicting the Attack Path of APT, Xupeng Fang, LidongZhai
5. Multi-Agent System for APT Detection,WimMees, ThibaultDebatty, Royal Military AcademyBrussels, Belgium
6. Incorporating the Human Element in Anticipatory and Dynamic Cyber DefenseAunshulRege, Department of Criminal Justice, Temple University, Philadelphia, USA
7. Moving Target Defense against Advanced PersistentThreats for Cybersecurity Enhancement, MasoudKhosravi-Farmad, Ali AhmadianRamaki and Abbas GhaemiBafghi, Data and Communication Security Lab., Computer Engineering Department, Ferdowsi University of Mashhad, Mashhad, Iran,
8. Shuffle-selective search, Abdul KhadarA, ShrishailMath, Srinivasamurthy, Published 2017
9. Analyzing Targeted Attacks using Hadoop applied to Forensic Investigation, Parth Bhatt, Edgar Toshiro Yano, Dept. of Electronics and Computer Engineering, InstitutoTecnológico de Aeronáutica,São José dos Campos,SP,Brasil,
10. https://attack.mitre.org/groups/G0045/
11. Detection ofvarious denial of service andDistributed Denial of Service attacks using RNNensemble, A. B. M. Alim Al Islam ; Tishna Sabrina,2009 12th International Conference on Computersand Information Technology, Year: 2009

AUTHORS PROFILE

Abdul Khadar A, M.Tech (CSE), Ph.DScholor, working as Assistant Professor in the department of ISE, SJCIT, Chickballapur, Karnataka, India.

Dr.ShrishailMath,Prof. Department of ECE, SKIT, Bangalore, Karnataka, India.Ph.D in Image Processing.

H Srinivasa Murthy, Associate Professor In the department of Computer Science and Engineering, SJCIT, Chickballapur, Karnataka, India.

Retrieval Number: A10170581C19/19©BEIESP

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication