International Journal of Engineering Applied Sciences and Technology, **2015, 1, 1-8**
Published Online June – July 2015 in IJEAST (http://www.ijeast.org/)

Review of Multistage Cyber Attack

Kuldeep Singh
Dept. of CS & E
Amity University
Noida, U.P, INDIA
lightningbolt275@gmail.com

Priyanka Singh
Dept. of CS & E
Amity University
Noida, U.P, INDIA
priyankasinghjan@yahoo.com

Pradeep Kumar Singh
Assistant Professor
Dept. of CS & E
Amity University
pksingh16@amity.edu

***Abstract*— with the increasing use of internet and networking devices, threat of the cyber attacks is also increasing. Group of specialist hackers are been higher by states and criminal organizations to spoil and steel the data of organizations. With the increase in the security systems, attackers have also come up with the new techniques and methods. Most affective and long term attack methodology at present is Multi Stage attacks which comprises of many sequential sub attacks at different levels. Each sub Attack has a specific task to perform. Multi Stage attack includes penetration followed by the removal of its traces, then searching of the victim's data to be manipulated or attack and then performing main task. These long Term Attacks are also termed as Advanced Persistent Attack (ATP). Organizations are investing a lot in their security system but still 95 % of them are the victims of these attacks.**

To tackle this type of attacks a simulation system can be implemented in which these attacks can be implemented and then studied. With that study, data can be generated which can be used for mapping of different types of Multi Stage attacks. This mapping is done by analyzing the network abnormal behavior if there is any.

Keywords— Multi Stage Attack, Advanced Persistent Attack, Penetration, Clustering and Cyber Attacks.

I. INTRODUCTION

Increasing use of internet and network devices, threat of the cyber attacks is increasing. As the most of the devices are open into the network with not much of security, there is always the chance of security Breach. Crackers and Hackers (Black Hats) are been higher by criminal organizations to spoil the data of legitimate organizations. Most effective attack technique now a days are DDoS and multi stage attacks which itself comprises of many sub attacks. Each sub Attack has a specific and fixed task to perform. First step of Multi Stage is penetration followed by the removal of it's traces, then searching of the victim's data to be manipulated or attack. These long Term Attacks with heavy damage are called as Advanced Persistent Attacks(ATP). Big Organizations like "Google" which have huge data bases are investing a lot in their security system but still many of them suffer from these attacks. Even if any single step gets failed then the whole attack may fail. But the attackers use these attacks quite proficiently. Hence has caused huge monitory and data loss to industry, people and nation.

II. MULTI STAGE ATTACK PATTERN

Today cyber attackers are incorporating different and advanced methodology in their attacks. Therefore, professional cyber analysts are being higher for monitoring the attack. Analysts see the attack according to its affect on the network. But, more information is there in its sub attacks. So, To tackle multi stage attacks analysts are working on the attack patterns of multi stage attack, patterns of sub attacks. With these attack patterns real big picture of attack can be predicted.

Few Attacks that are the part of multi stage attack are:-

- Call of Action
- Recruitment
- Intelligence Gathering
- Vulnerability Scanning
- Defacement
- Steal Information
- Mass DOS Attack

III. APPROACHES TO TACKLE

a. In [1], Clark D.D *et al* discusses the reason for network level personal attribution is of very limited forensic

importance. He analyzes and focuses on the different types of attacks based on internet, and observes the role and performance of currently available alternatives to attribution plays in preclusion and prosecution. We can't design the Network system again because it will cost very a lot. So, instead of alternating the network system focus should be on other approaches, like as making multi stage cyber attacks more difficult, resource consuming and costly. And, instead of issuing the calls for better attribution on the network, such applications should be designed that can do better job of integrating identity.

b. In [2], S. Mathew *et al* presented a method of handling the visualization of heterogeneous event traffic that is created by intrusion detection sensors, log files and other event sources on a computer network from the point of view of detecting Multi Stage Attack paths that are of importance. Aggregation and correlation of these events based on their Semantic content to generate Attack Tracks that are displayed to analyst in the real time. The tool used here is Event correlation for cyber attack Recognition System. Testing of this system indicates the correlation and visualization of heterogeneous network events in the context of multistage attacks adds significant value to the practice of cyber attack detection.

$$\text{Precision} = \frac{\text{Number of True Positives}}{\text{Number of True Positives} + \text{Number of False Positives}}$$

$$\text{Recall} = \frac{\text{Number of True Positives}}{\text{Number of True Positives} + \text{Number of False Negatives}}$$

c. In [3], S. Mathew *et al* discusses the Correlation and fusion of intrusion alerts to provide effective situation awareness of the cyber attacks and it is very much accepted by research teams in this field. Snort is the most widely used Intrusion Detection sensor. For security, admin snort is the primary indicator of the network misuse. He discusses an Attack stage oriented classification of alerts using snort in his paper. Classification of intrusion detection sensor alerts is done based on their role as the part of goal oriented multi stage attacks. This approach improves the real-time awareness for the multistage attack.

In his paper he presented a scheme of classification of intrusion detection alerts based on their roles. Further IDS sensors alerts can be incorporated into the scheme for better detection of Multistage Attacks and this way system can be made more robust.

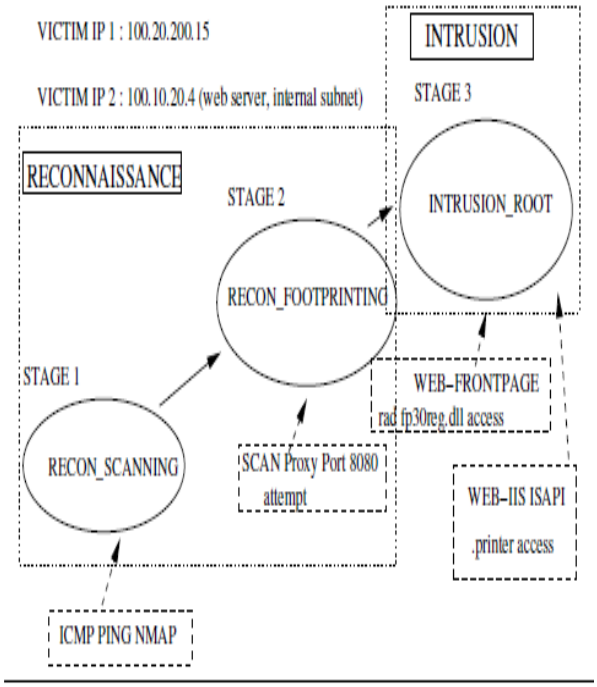

Fig: 1 Effective Attack Awareness indicating attack stage progression [3].

d. In [4], M. Alnas *et al* discusses the Network Intrusion Detection Systems (NIDS) are considered as one of the essential mechanisms to ensure reliable security. Detection of novel and multi-stage attacks are not efficiently achieved by the signature-based systems. Hence, the systematic analysis of attack initiation has become a stressing demand in current research. Correlation of Alerts techniques have been widely used to provide intelligent and stateful detection methodologies. In his paper the limitations of the present techniques and model for correlation for the alerts have been identified that overcomes the weaknesses. An improved "require/provide" model is presented which established cooperation between statistical and knowledge-based model, to achieve higher detection rate with the minimal false positives. This methodology is been implemented in an isolated environment to tackle the most dangerous problems that is bot-nets.

International Journal of Engineering Applied Sciences and Technology, 2015, 1, 1-8
Published Online June – July 2015 in IJEAST (http://www.ijeast.org/)

Algorithm:

Input: elementary alerts generated by the IDS
Output: Correlated Attack Graph *CAG (N,G)*
Methods:

1- Let CAG (N,G) = null

2- Map elementary alerts to M-Alerts instances ($m_0, m_1, \ldots, m_i$)

3- Let m_0 an instance of isolated M

4- For k=1 to i

If a. at least one $R(m_{i+1}) \sqsubset P(m_i)$
$\sqsubset R(m_{i+1}) \sqsubset EP(m_i)$
b. V(m_{i+1}), V(*m*), EX(m), and D(m) are satisfied.
c. P(mi).End_time >= R (m_{i+1}).Start_time
$\sqsubset$ EP(mi).End_time >= R (m_{i+1}).Start_time
Then
Add CAG (nm_i, nm_{i+1})
5- Return CAG (N,G)

IV. In [6], S.J Yang *et al* say that Current methodologies to fight against cyber attacks are typically reactive yet non resistive. Recent research work has come up with techniques which can predict hacker's target machines in the early stage of the attack. Though predictions can be made regarding the attack but still false prediction can happen. Very little had been researched about how to evaluate an algorithm for threat assessment. With the increasing attacks, a threat assessment algorithm will be more susceptible. But still the lack of database is perhaps the part of very reason why little can be found about assessment of cyber attack. So, it is suggested that different mixtures of methodologies has to be selected or taken to tackle normal and abnormal cyber-attacks.In [7], D. Shen *et al* proposed level based methodology in which alerts generated by Intrusion Detection Sensors (IDSs) or Intrusion Prevention Sensors (IPSs) are put into the data refinement which is at level 0 and object assessment which is at level 1. Markov game model is used for High-level situation/threat assessment (L2/L3). To refine the primitive prediction generated by adaptive feature/pattern recognition, Hierarchical Entity Aggregation is proposed and further captures new unknown features. To estimate the belief of each possible cyber attack pattern a markov game method is used. Game theory can capture the nature of cyber conflicts: determination of the attacking-force strategies is tightly hold together.

Also, Markov game theory deals with uncertainty and incompleteness of available Information.

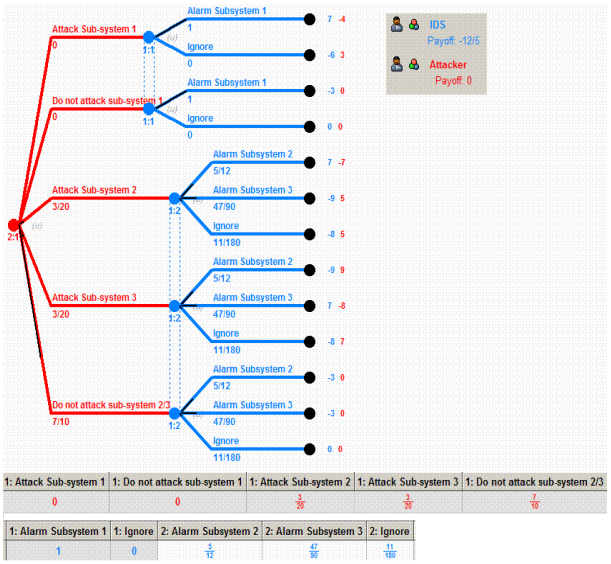

Fig 2: An Example of Decision Support Based on static matrix game model [7].

e. In [8], F.A Bahareth *et al* say that with the increase in attacks the alerts generated against the attack is also iincreasing.

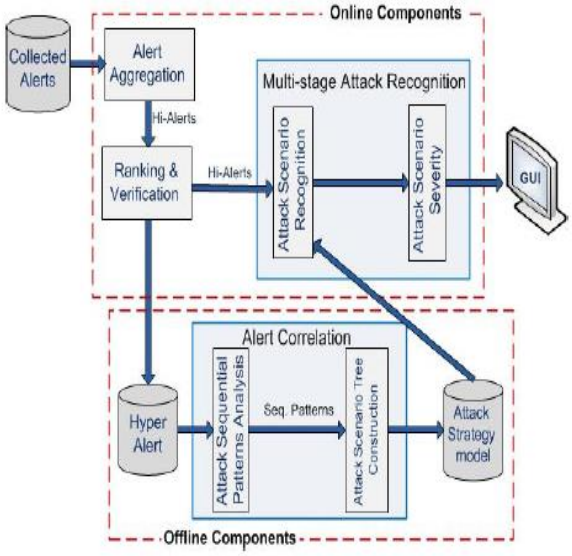

Fig 3: Proposed Solution Framework [8].

The number of alerts generated has started to become the problem. To tackle these attacks plus the alerts generated with the attacks, attack correlation methodology is been

accepted which will set up the alert correlation which can result in attack. This way the number of alerts can be decreased. Sequential mining algorithm is used to find out the attack pattern. To improve the efficiency of this methodology, the candidate verification that calculates alert correlativity while generating candidate attack sequence should is done .

f. In [9], H. Wang *et al* discusses that IP Spoofing has mostly exploited by Distributed Denial of service. Attacker uses different slave machines to attack the victim for their malicious activities. They can manipulate many attributes in the network to deceive the admin and network security but they can't alter one thing that is Hop Count traveled to reach the target machine.

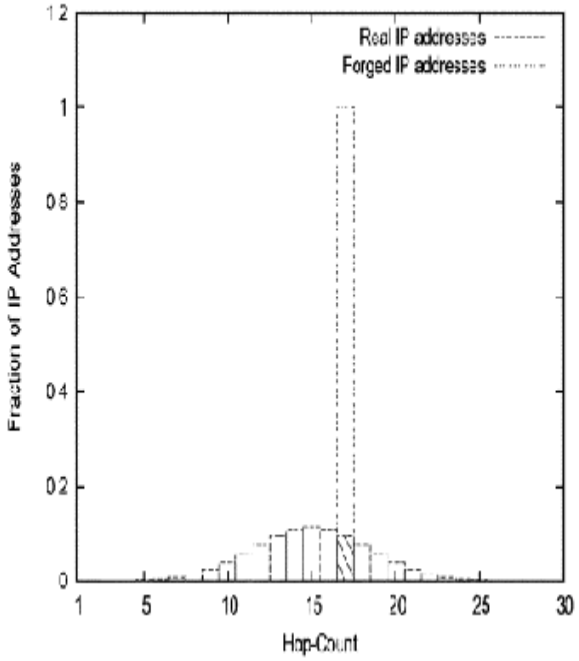

Fig 4: Hop count distribution of IP addresses with a single flood source [9].

Hop count is the number of intermediate machines a data packet has traveled to reach its destination machine. Maximum number of Hop Count a data packet can have is 16. Hop count can be calculated by deducting 1 from TTL value each time data packet traveled to intermediate machines before reaching the final machine. In this paper Hop count is used to detect whether the request is coming from some legitimate user or from some attacker. In the beginning the system will be in the learning stage to know the resources accessed by the users and then later creating the graph of Ip addresses against the Hop Count. Based on this chart system can differentiate valid user and attacker.

Hop count = TTL(Initial) – TTL(final)

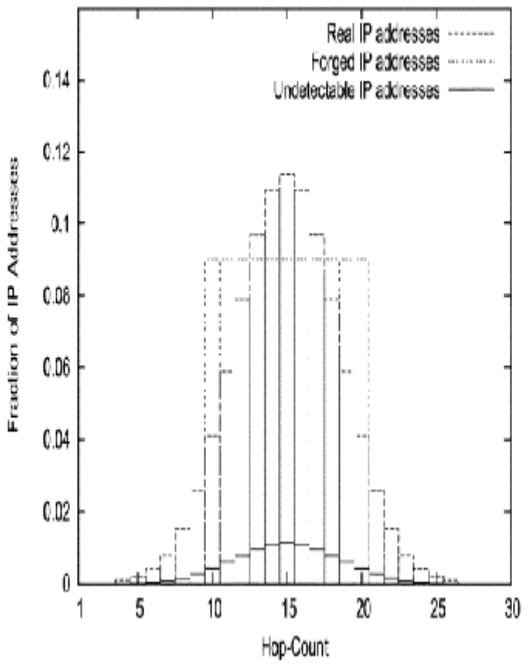

Fig 5: Hop Count Distribution of IP addresses with a single source, randomized TTL [9].

g. In [10], S. Xin *et al* discusses that Distributed Denial of service attack is very effective and important part of the multistage attack. Many servers efficiency get reduced from its normal efficiency to low because of this type of attack. But, all the multistage attacks can be subdivided into sub attacks. When these attacks complete their task for which they are designed then only whole attack will get successful. So, A learning engine can be designed which will be having the knowledge of different types of combination possible of the atomic attack with high proximity for the cyber attack. And, Base upon those

combinations the attacks can be identified and then tackled within the time with least possible loss.

V. CONCLUSION

On the basis of above discussion conclusion can be made that multi stage attack cannot be tackle with the normal methods. So, An adaptive model can be made related to this type of attack which will generate the attack alerts based on the previous data of the attacks. As In multistage attack attackers flush the victims with heavy DOS attacks, there will be enormous amount of alerts that will get generate. So, An attack correlation system should be there in the system that will generate the alerts for those attack patterns only which can really result in some attack and its consequence.

VI. FUTURE SCOPE

This methodology can further be refined with the help of more data base regarding the attack sequence possible in case of multi stage attack. That data base will be use to train the system and this will further be useful in predicting the attacks techniques, patterns and then at some point most of the possibilities can be considered and most possible attacks can be tackled.

References

[1] Clark D.D, Landau S. "The Problem is not the Attribution; It's Multi Stage Attack", ACM, pp. 4503 , 2010.

[2] S. Mathew, R. Giomundo, S. Upaadhyaya, M. Sudit, A. Stotz, "Understanding Multistage Attacks by Attack-Track based Visualization of Heterogeneous Event Streams", ACM, pp. 549, 2006.

[3] S. Mathew, R. Giomundo, S. Upaadhyaya, M. Sudit, A. Stotz, "Real- Time Multistage Attack Awareness Through Enhanced Intrusion Alert Clustering", ACM, 2006.

[4] M. Alnas, A.M. Hanashi, E.M. Laias, "Detection of Botnet Multi-Stage by Using Alert Correlation Model", IJES, 2013.

[5] Symantec Report, "Protecting POS Environment Against Multi-Stage Attacks", Semantec Intelligence Report, 2013.

[6] S.J. Yang, J. Holsopple, M. Sudit, "Evaluating Threat Assessment for Multi-Stage Cyber Attacks".

[7] D. Shen, G. Chen, J. B. Cruz, L. Haynes, M. Kruger, E. Blasch, "A Markov game Theoretic Data Fusion Approach for Cyber Situational Awareness", Office of Naval Research, 2007.

[8] F. A Bahareth, O. O. Bamasak, "Constructing Attack Scenario Using Sequential Pattern Mining with Correlated Candidate Sequences", ACM, 2013.

[9] H. Wang, C. Jin, K. G. Shin, "Defense Against Spoofed IP Traffic Using Hop-Count Filtering", IEEE/ACM, 2007.

[10] S. Xin, X. Chen, H. Tang, N. Zhu, "Research on DoS Attack Oriented to Attack Resistance Test", ICNSC, 2007.

[11] D. Fava, J. Holsopple, S. J. Yang, B. Argauer, "Terrain and Behavior Modeling for Projecting Multistage Cyber Attacks"

[12] R. Katipally, W. Gasior, X. Cui, L. Yang, "Multi Stage Attack Detection System for Network Administrators Using Data Mining"

[13] Z. Duan, X. Yuan, J. Chandrashekar, "Controlling IP Spoofing Through Inter-Domain Packet Filters" IEEE, 2006.

[14] Y. Chen, W. Trappe, R.P. Martin, "Detecting and Localizing Wireless Spoofing Attacking".

[15] Y.Chen, K. Hwang, W. S. Ku,"Collaborative Detection of DDoS Attacks Over Multiple Network Domains".

[16] "Lets Talk Security", [Online]. Available: http://letstalk.globalservices.bt.com/en/security/2013/08/multi-stage-attack-modelling-your-new-weapon-against-sophisticated-cyber-attacks/ last accessed on 12-10-2014.

[17] "ACM Digital Library", [Online]. Available: http://dl.acm.org/citation.cfm?id=1179578/ last accessed on 12-10-2014

[18] "Springer Link", [Online]. Available: http://link.springer.com/chapter/10.1007%2F978-3-642-33469-6_37/ last accessed on 12-10-2014.

[19] "Incapsula", [Online]. Available: http://www.incapsula.com/ddos/ddos-attacks/ last accessed on 12-10-2014.

[20] "MIT Technology Review", [Online]. Available: http://www.technologyreview.com/view/528861/cyber-attacks/ last accessed on 13-10-2014.