Condition for Blocking
$\alpha = \sum \beta(x)$
Where α is the Response of the system
β is the suspicious list In terms of x (IP data or packet header of the request in particular Time)
Else
Statement: Allow the Request to Process.

3.3 Characterize the threat models –Unsupervised (unlabelled)

Novel Threats in the network and host system is difficult to detect. To enable the novel attack detection set of attributes from each event (IP packet or TCP connection), including strings in the payload, and induce a set of conditional rules which have a very low probability of being violated in a no stationary model of the normal network traffic in the training data.

Figure 4.4: Botnet Propagation in the Network

3.4 Learning Rules for Anomaly Detection

We extend the network traffic model to include a large number of attributes, including the application payload. We introduce a non stationary model, in which the probability of an event (an attribute having some value) depends on the time of its most recent occurrence, and not on its average frequency. We introduce an efficient algorithm for selecting good rules for anomaly detection from a rule space that is exponentially large in the number of attributes.

3.5 Attack Correlation based on the Vulnerability Ratio and Attack Strategies:

Vulnerability of networks is been estimated through considering the geometric properties of regional failures and network nodes. To evaluate the criticality of node locations and determine the critical areas in a network, we propose the concept of α-critical-distance with a given failure impact ratio α, and we formulate two optimization problems based on the concept. By analyzing the geometric properties of the problems, we show that although finding critical nodes or links in a pure graph is a NP-complete problem, the problem of finding critical areas has polynomial time complexity. We propose two algorithms to deal with these problems and analyze their time complexities. Additionally, we find that with the same impact ratio α, the topologies examined have larger α-critical-distances when the network performance is measured using the giant component size instead of the other two metrics. Similar results are obtained when the network performance is measured using the average two terminal reliability and the network efficiency, although computation of the former entails less time complexity than that of the latter

3.6 Developing the flow based Clustering Technique as Detection Technique

Cluster is been utilized for parallel detection in order to increase the detection speed in large networks.

3.7 Developing a PSO based Clustering Technique as detection Technique

Particle has taken time or identity or data or file. Velocity has been no. of occurrence in specified time. It measures the type of the file and size of file of same content or data.

4. Experimental Results

We evaluated the system against botnet and DDOS attacks with screens as follows. All but a few attacks show some evidence in the inside network traffic, so to simplify the results we just report all detections.

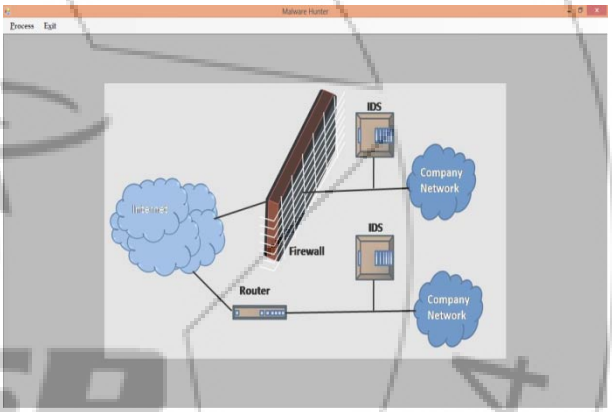

Figure: Overall process outlet Screen

We expected to prove the proposed solution, thus achieving our goal "establish dynamic defensive mechanism-based software defined networking approach that involves multiphase intrusion detections.

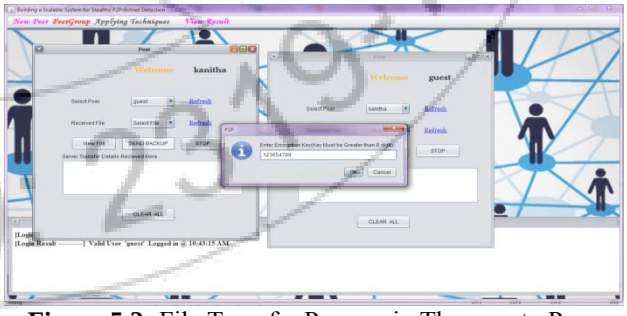

Figure 5.2: File Transfer Process in The peer to Peer Networks

The Data Communication by the BotNet attacks is shown as follows

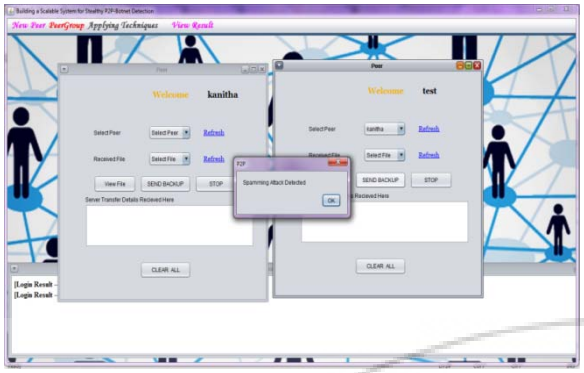

Figure 5.3: Spam Detected in the file transferring by the BOTMASTER

In each concerned system call, we set up one or more checkpoints, each of which is responsible for checking the behaviors belonging to the same operation with the support of a modifiable behavior list in memory.

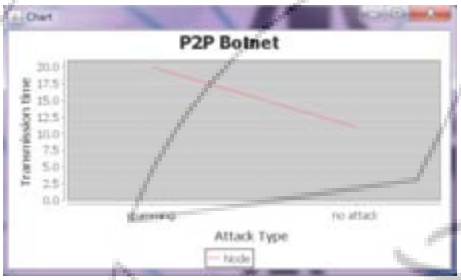

Figure: Detection Accuracy of the Malware Seeker for PEER to PEER BOTNET

The performance results provide us a benchmark for the given hardware setup and shows how much traffic can be handled by using a single detection domain.

Data Recovery Process

Figure: Rate of Successful data recovery

To scale up to a data center-level IDS, a decentralized approach must be devised. We utilized the synthesis data for the experimental evaluation and proposed a multiple technique random traffic data and Experimental results has been derived.

5. Conclusion and Future Work

We implemented a multiphase distributed vulnerability detection through the Principle of component analysis of each traffic data under the dynamic attack evolution area, measurement and countermeasure selection mechanism called Malware Hunter which is built on attack graph-based analytical models based on classification process and reconfigurable against update solutions to virtual network-based countermeasures. The classification process has been carried using the principle component analysis to establish the efficient detection mechanism against the attacks. The System has been included with different characters for modeling with attack detection solutions for botnet attacks. The proposed framework leverages hierarchical models to build a monitor and control process to classify the network traffic data to the virtual machine to significantly improve attack detection and mitigate attack consequences. Hence malware hunter achieves the good detection performance against all types of network and host based intrusion evolving. As a future work, We introduce novel Solution to mitigate the malicious activities of Botnet attackers through the detection mechanism and countermeasure strategies .To prevent vulnerable virtual machines from being compromised in the cloud, we propose a multiphase distributed vulnerability detection for each traffic data, measurement and countermeasure selection.

Reference

[1] S. Stover, D. Dittrich, J. Hernandez, and S. Dietrich, "Analysis of the storm and nugache trojans: P2P is here," in *Proc. USENIX*, vol. 32.2007, pp. 18–27.

[2] P. Porras, H. Saidi, and V. Yegneswaran, "A multi-perspective analysis of the storm (peacomm) worm," Comput. Sci. Lab., SRI Int., Menlo Park, CA, USA, Tech. Rep., 2007.38 IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 1, JANUARY 2014

[3] P. Porras, H. Saidi, and V. Yegneswaran. (2009). *Conficker C Analysis*[Online].Available: http://mtc.sri.com/Conficker/addendumC/index.html

[4] G. Sinclair, C. Nunnery, and B. B. Kang, "The waledac protocol: The how and why," in *Proc. 4th Int. Conf. Malicious Unwanted Softw.*, Oct. 2009, pp. 69–77.

[5] R. Lemos. (2006). *Bot Software Looks to Improve Peerage* [Online] Available: http://www.securityfocus.com/news/11390

[6] Y. Zhao, Y. Xie, F. Yu, Q. Ke, and Y. Yu, "Botgraph: Large scale spamming botnet detection," in *Proc. 6th USENIX NSDI*, 2009, pp. 1–14.

[7] G. Gu, R. Perdisci, J. Zhang, and W. Lee, "Botminer: Clustering analysis of network traffic for protocol- and structure-independent botnet detection," in *Proc. USENIX Security*, 2008, pp. 139–154.

[8] T.-F. Yen and M. K. Reiter, "Are your hosts trading or plotting? Telling P2P file-sharing and bots apart," in *Proc. ICDCS*, Jun. 2010, pp. 241–252.

[9] S. Nagaraja, P. Mittal, C.-Y. Hong, M. Caesar, and N. Borisov, "BotGrep: Finding P2P bots with structured graph analysis," in *Proc. USENIX Security*, 2010, pp. 1–16.

[10] J. Zhang, X. Luo, R. Perdisci, G. Gu, W. Lee, and N. Feamster,"Boosting the scalability of botnet detection using adaptive traffic sampling," in *Proc. 6th ACM Symp. Inf., Comput. Commun. Security*,2011, pp. 124–134.

[11] J. Zhang, R. Perdisci, W. Lee, U. Sarfraz, and X. Luo, "Detecting stealthy P2P botnets using statistical traffic fingerprints," in *Proc.IEEE/IFIP 41st Int. Conf. DSN*, Jun. 2011, pp. 121–132.

[12] S. Saad, I. Traore, A. Ghorbani, B. Sayed, D. Zhao, W. Lu, *et al.*, "Detecting P2P botnets through network

behavior analysis and machine learning," in *Proc. 9th Annu. Int. Conf. PST*, Jul. 2011, pp. 174–180.
[13] D. Liu, Y. Li, Y. Hu, and Z. Liang, "A P2P-botnet detection model and algorithms based on network streams analysis," in *Proc. IEEE FITME*, Oct. 2010, pp. 55–58.
[14] W. Liao and C. Chang, "Peer to peer botnet detection using data mining scheme," in *Proc. IEEE Int. Conf. ITA*, Aug. 2010, pp. 1–4.
[15] T. Karagiannis, K. Papagiannaki, and M. Faloutsos, "BLINC: Multilevelm traffic classification in the dark," in *Proc. ACM SIGCOMM*, 2005, pp. 229–240.
[16] S. Sen, O. Spatscheck, and D. Wang, "Accurate, scalable in-network identification of P2P traffic using application signatures," in *Proc. 13th ACM Int. Conf. WWW*, 2004, pp. 512–521.
[17] T. Karagiannis, A. Broido, M. Faloutsos, and K. Claffy, "Transport layer identification of P2P traffic," in *Proc. 4th ACM SIGCOMM Conf. IMC*, 2004, pp. 121–134.