Abstract

Cyber attacks have been a part of modern human combat. Various technologies like Intrusion detection system (IDS), Intrusion Prevention system (IPS), firewalls are under active monitoring to generate alerts and in preventing cyber-attacks. However, these mechanisms are not the solutions as they cannot generate accurate solutions, potentially Intrusion detection system tend to generate false signals. Perhaps, cyber attacks cannot be just controlled with just tools. Instead it requires an Indicator of compromise (IoC) which is an important subject in IT sector to identify true positive attacks. In this paper, it is proposed a new threat intelligence technique which evaluates by analysing honeypot’s log data to identify true cyber attacks and to immediately act an incident response process. This goal is achieved by deploying a honeypot on an AWS cloud to gather cyber-attacks. This method of malware bypasses technical solutions by leveraging social engineering methods in order to prevent ransomware attacks. An additional system for perimeter defence is established. Honeypots are spurious computer resources deployed by network administrator to act as decoy computers and identify any informal access.
Honeypots: Screening Cyber Attacks

Investigations determined a suitable method to identify changes to this aspect. Two options were filed under research, one is the file screening service of the Microsoft File Server Resource Manager feature and the other is Event Sentry to manipulate the Windows Security logs. Under development process, a determined response to attacks to the system along with threshold were initiated. The research also mentioned that witness to tripwire files offered limited value as there is no alternative to influence the malware to access monitored files.

References

1. Adnaan Arbaaz Ahmed, Dr. M.I. Thariq Hussan, “Cloud Computing: Study of Security Issues and Research Challenges”, International Journal for Advanced Research in Computer Engineering and Technology Volume 7, Issue 4, 362-369, April 2018.
2. Adnaan Arbaaz Ahmed, Durganath Rajesh, Dr. M.I. Thariq Hussan, “Implementing Machine Learning Techniques in Malware Detection”, International Journal for Research in Engineering Application and Management Volume 4, Issue 9, 155-158, December 2018.
3. Adnaan Arbaaz Ahmed, Dr. M.I. Thariq Hussan, Venkateswarlu Bollapalli, “Upgrade - Data Security in Cloud by Machine Learning and Cryptography Techniques”, International Journal of Engineering and Advanced Technology Volume 8, Issue 6, 2728-2732, August 2019.
4. Navneet Kambow, Lavleen Kaur Passi, “Honeypots: The Need of Network Security” International Journal of Computer Science and Information Technologies, Vol. 5 (5), 2014, 6098-6101
5. Pavol Sakol, Jakub Misek, Martin Husak, “Honeypots and honeynets: issues of privacy” EURASIP Journal on Information Security, February 2017
6. AUTHORS PROFILE
7. Adnaan Arbaaz Ahmed popularly known as Technophyle Ahmed is a tech junkie and a self proclaimed offensive and defensive ethical hacker and security expert of computer systems. He is specialized in Networking, Cloud Computing, Linux, Java, Python, Ethical Hacking, Cyber Security, Machine Learning, Artificial Intelligence, DevOps, Data Science, Containers Technology, Blockchain, etc. He is the director of Techionary. He delivered almost a 50 workshops on the above listed domains igniting young minds with advancements in Technology. He has four international publication out of which two are industrially implemented. Life time member of World Research Council. Honored with the title Research Ratna 2019 as the Best Researcher in Information Technology by RULA Awards.
8. Vanam Rajkumar, is the Chief of Executive of Techionary. Speaker for Institute for Engineering research and Artificial Intelligence (IERAI-2020) for the topic “AI assisted chatbot for visually impaired and disabled persons”. Member of International Association of Engineers society of Artificial Intelligence (IAENG). Project fellow at Foundation for Advancements In Engineering and Research (FAER-2019) for the proposal titled “Detection of harmful gas to ensure safety and security of human life and property.”
9. Dr. M.I. Thariq Hussan has 18 International and 1 National journal publications. He has presented papers in 31 International/National conferences and attended 36 Seminars/Workshops/FDP/QIP. He has published 2 books titled ‘System Analysis and Design’ and ‘Operating Systems’. He has received ‘Innovative Technological Research (Communication) and Dedicated Professor Award’ from Innovative Scientific Research Professional Malaysia (India Chapter). He also received ‘Best Teacher Award-2018’ from Institute for Exploring Advances in Engineering accredited by EA-JAS. He has filed 2 patents
Honeypots: Screening Cyber Attacks

titled ‘Vision Based Safety Seat Belt Monitoring System’ and ‘Intelligent Detect and Control Cybercrime Device’. He has qualified ESOL certificate in English by Cambridge University. He is a life member of ISTE and nominee member of CSI for knowledge exchange and enhancement.

**Index Terms**

Computer Science  
Security

**Keywords**

AdbHoney, Amun, Artilliary, AWS, CiscoASA, Cowrie, Conpot, Cyber Attacks, Cyber Security, Dianaea, EC2, Elastic Pot, Elastic Search, Glastopf, Glutton, Herald, Honeypie, Honeypots, Honeytrap, Kibana, Kippo, LogStash, Mailoney, P0f Engineering tool, Port Forwarding, Port Numbers, Rpsy, Security, Server logs, Snare, Tanner