Proposal 3

Instigators: Abderrahim Benslimane and Julio Perez, Avignon University, France

Title: Automatic identification of malicious activities by monitoring Darknet Network

Summary of the proposal

The Internet has become highly integrated into our current everyday lives. Society has gone digital through communication, socializing, learning and doing business online. Furthermore, in order to improve the quality and efficiency of work, governments are leveraging the Internet to operate their critical infrastructure. While cyberspace provides major benefits, our increasing reliance on it is producing new, significant vulnerabilities. As such, any security breach has the potential to result in debilitating effects on security, economy, public health, or safety. In addition, cyber attacks are dramatically increasing in size and number. Recent online threats demonstrated that organizations and governmental agencies could be subjected, nearly instantaneously and in full anonymity, to large-scale disrupting and orchestrated attacks with the potential to lead to severe security, privacy, and economic consequences (i.e. cyber-terrorism, DDoS (Distributed Denial of Service), DRDoS(Distributed Reflection Denial of Service), information theft, spam and fraud) [1]. Darknet network have been used for years as a source of information for cybersecurity. A darknet is a set of IP addresses advertised by routing protocols, however without hosting any device [2].

In this project we will propose an architecture that allow to collect traffic with the differently located darknet sensors considering parameters such as traffic pattern, protocols, targeted port (destination port) and use the collected data to train different Machine Learning classifiers. This may further help in to understand topological behaviors of darknet traffic and detect possible attacks in the network (i.e. DDoS, Probing activities). In addition, create new datasets could provide some additional important information or reconfirmation of previous findings.

Our goal in this project is to use the traffic collected on the Darknet to train a Machine Learning algorithm to detect possible attacks on the network.

Related Work

Usually darknets receive traffic only for one of three reasons: traffic sent accidentally/by mistake, backscatter, malicious activity of scanning and worms. Accidental Darknet requests can occur if an individual mistyped an IP address or the URL used had an incorrect Domain Name Service (DNS) entry leading to a darknet. To hide identity of sender, DoS attacks are launched using Spoofed IP address. All traffic reaching the darknet remains unanswered and, by definition, is considered unsolicited. A monitoring probe or darknet sensor listens to the darknet traffic, processing it in search for signals of new threats, misconfigurations and possibly sources/victims of attacks [3].

There is a lack for automatic ways to uncover correlations among different events, which could help reducing the manual work when interpreting darknet traffic [4]. A promising approach is to apply Machine Learning (ML) using supervised learning to train a threat detection system using malicious and normal traffic. Some authors have proposed the utilization of Machine learning algorithms to detect DoS and probing attacks [5-7].

Plan

- Study the state of the art in Darknet sensor and comparing the different existing architectures.
- Select adequates Machine Learning algorithms to classify (detect) the different attacks (e.g. DDoS, RDoS, Probing, etc).
- Get familiar with sniffing softwares (i.e. Wireshark) and with pentesting and probing tools (i.e. Kali Linux tools, Ethercap, DDoSIM (DDoS Simulator), nmap, etc).

The three tasks above should be done **before the first day of the internship**.

- Implementation of the darknet sensor and launch different attacks againt a victim computer and collect the traffic.
- Train the machine learning algorithms with the collected traffic and compare the performance using the confusion matrix.
- Final report.

REFERENCES

[1] C. Fachkha and M. Debbabi, “Darknet as a Source of Cyber Intelligence: Survey, Taxonomy, and Characterization,” *IEEE Commun. Surv. Tutorials*, vol. 18, no. 2, pp. 1197–1227, 2016, doi: 10.1109/COMST.2015.2497690.

[2] F. Soro, I. Drago, M. Trevisan, M. Mellia, J. Ceron, and J. J. Santanna, “Are darknets all the same? On darknet visibility for security monitoring,” *IEEE Work. Local Metrop. Area Networks*, vol. 2019-July, 2019, doi: 10.1109/LANMAN.2019.8847113.

[3] P. S. Joshi and H. A. Dinesha, “Survey on identification of malicious activities by monitoring darknet access,” *Proc. 3rd Int. Conf. Smart Syst. Inven. Technol. ICSSIT 2020*, no. Icssit, pp. 346–350, 2020, doi: 10.1109/ICSSIT48917.2020.9214121.

[4] F. Soro, M. Allegretta, M. Mellia, I. Drago, and L. M. Bertholdo, “Sensing the Noise: Uncovering Communities in Darknet Traffic,” *2020 Mediterr. Commun. Comput. Netw. Conf. MedComNet 2020*, 2020, doi: 10.1109/MedComNet49392.2020.9191555.

[5] P. S. Joshi and H. A. Dinesha, “Survey on identification of malicious activities by monitoring darknet access,” *Proc. 3rd Int. Conf. Smart Syst. Inven. Technol. ICSSIT 2020*, no. Icssit, pp. 346–350, 2020, doi: 10.1109/ICSSIT48917.2020.9214121.

[6] Z. Wang, W. Cheng, and C. Li, “DoS attack detection model of smart grid based on machine learning method,” *Proc. 2020 IEEE Int. Conf. Power, Intell. Comput. Syst. ICPICS 2020*, pp. 735–738, 2020, doi: 10.1109/ICPICS50287.2020.9202401.

[7] S. Kumar, H. Vranken, J. Van DIjk, and T. Hamalainen, “Deep in the Dark: A Novel Threat Detection System using Darknet Traffic,” *Proc. - 2019 IEEE Int. Conf. Big Data, Big Data 2019*, pp. 4273–4279, 2019, doi: 10.1109/BigData47090.2019.9006374.