**Final Year Project Proposal**

|  |  |  |  |
| --- | --- | --- | --- |
| Sr# | Student Name | Roll Number | Signature |
| 1 | Muhammad Affan Khan | 19P-0045 |  |
| 2 | Rana Rehan Qaisar | 19P-0077 |  |
| 3 | Istafa Malik | 19P-0033 |  |

**Suggested Supervisor**:

Faculty Member’s Name: Muhammad Amin Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date (01 January 20XX)

**Project Details**

|  |  |  |  |
| --- | --- | --- | --- |
| **Project Title** | Combating Crypto-jacking through Machine Learning-Based Network Traffic Analysis | | |
| **Project Area of Specialization** | Cyber security and Machine Learning | | |
| **List Related Core Subjects** | 1) Information Security  2) Artificial Intelligence  3) Operating Systems  4) Parallel and Distributed Computing | | |
| **List Related Elective Subjects** | 1) Machine Learning  2) Data Science  3) Data Mining | | |
| **Project Start Date** | 2023-02-05 | **Project End Date** | 2023-12-31 |
| **Project Summary (less than 2500 characters)** | There is a novel cyber security attack where an adversary silently runs crypto-mining software over the devices of unaware victims, both in literature and in reality. The success of this assault, often known as "crypto-jacking," can be attributed to how simple it is to install a crypto client on a target device. A host-based architecture combines a variety of recently created countermeasures with different traits and capabilities. A corporate network cannot be successfully secured with this kind of user protection solution, especially from insider threats. In the present study, we propose a network-based approach for detecting and recognizing crypto-client behaviors using only the network traffic, even when it is encrypted. In the beginning, we give a thorough analysis of the real network traces generated by three important crypto currencies, Bitcoin, Monero, and Bytecoin, while accounting for both conventional traffic and VPN-shaped traffic. We then show Crypto-Aegis, a Machine Learning (ML) based system built to identify crypto currency-related behaviors such as active full nodes, pool mining, and solo mining, based on the results of our investigation. | | |
| **Project Objectives (less than 2500 characters)** | 1) Crypto jacking Analysis  2) Crypto jacking Detection | | |
| **Project Implementation Method (less than 2500 characters)** | We examine a business network made up of numerous linked devices, including one that is under the authority of an evil entity and eager to mine bitcoins covertly detected. Our solution just requires an Ethernet connection from the primary Corporate Network switch to a server running our Machine Learning algorithm, and it should be implemented at the network edge. We note that neither staff devices nor the pre-existing network infrastructure needs to be modified to use our solution. Deploying numerous Ethernet lines to gather the data from the Corporate Network exit points makes it simple to deploy our solution even when there are several exit connections between the Corporate Network and the Internet. We note that the aforementioned configuration is extremely restrained in comparison to common commercial options. Corporate solutions typically entail hardware for deep packet inspection installed before the exit point or even at several different network sites. The relationship between traffic and gadget is one thing but is simpler, but on the other hand, it costs a lot to deploy and buy the necessary hardware. We take into account the already-aggregated traffic in our solution, i.e., impacted by NAT or IP masked, or even tunneled and by a Virtual Private Network to be re-encrypted (VPN). | | |
| **Benefits of the Project (less than 2500 characters)** | Machine learning algorithms are capable of analyzing network traffic in real-time so businesses are able to identify and stop crypto-jacking attempts.  Compared to manual analysis, Machine Learning systems may detect crypto-jacking more quickly and with less effort by automating the process.  Compared to conventional security solutions, machine learning algorithms are capable of evaluating enormous amounts of data and spotting patterns, which lowers the possibility of false positives and negatives.  By improving security, reducing resource consumption and increasing efficiency, machine learning based network traffic analysis can help organizations save on operational costs and avoid the financial losses associated with crypto-jacking attacks.  Machine learning algorithms are flexible to the continuously changing threat landscape of crypto-jacking attempts because they can learn from new patterns and develop over time.  To provide a greater defense against crypto-jacking assaults and other security risks, ML-based network traffic analysis can be used in conjunction with other security measures. | | |
| **Technical Details of Final Deliverable (less than 2500 characters)** | We will develop a software that will use a ML-Based Algorithm and will perform traffic analysis on a single computer. It will prevent crypto Jacking by analyzing the traffic and will generate a warning and will give an option to block the hacker’s IP. | | |
| **Final Deliverable of the Project** | The final product should be a reliable and expandable solution that easily fits into the organization's network infrastructure and offers continuous defense against crypto-jacking attempts. | | |
| **Type of Industry** | 1. Cyber security 2. Artificial Intelligence 3. Information Technology 4. Blockchain | | |
| **Technologies** | 1. Machine Learning 2. Network Traffic Analysis | | |
| **Sustainable Development Goals** | The project's overarching goal is to give enterprises a secure and effective network environment by quickly identifying and stopping crypto-jacking activity without interfering with regular network operations. The solution should offer a complete approach to thwarting crypto-jacking and be scalable, user-friendly, and simple to incorporate into current network architecture. | | |

**Project Key Milestones**

|  |  |  |
| --- | --- | --- |
| **Elapsed time in (days or weeks or months or quarters) since the start of the project** | **Milestone** | **Deliverable** |
| Month 1 | 1st 6 Months | Working prototype for traffic analysis using ML |
| Month 2 | 2nd 6 Months | Software application for traffic analysis and prevention of crypto jacking. |