Research Plan

The increase of the number of malware has been going rapidly. According to AV-Test report, in 2021 the number of malware totaled around 1250 million, a 12 times increase of that of 2012, which was around 100 million [1]. As the increase of the total amount of malware has increased, malware types and new attack methods are created and evolving by the day.

Most types of modern malware communicate with external servers using different network protocols, where DNS(Domain Name Server) services are used most frequently. These malware often are using DNS Services to locate a C & C (command and control) servers instead of using fixed IP addresses [3]. In particular, these malware uses DGA(domain generated algorithm) to generate domain names to avoid tracking. As a single domain or a fixed IP address can be easily tracked. These malicious domain names will then be put in a blacklist, which would make those domain names not accessible anymore. While malware that uses DGA connect to malicious domain names, which are active for a limited amount of time. This prevents them to being blocked by blacklist-based countermeasures. The domain names generated by the DGA are registered in advance to secure those generated domain names.

When a domain name is detected and blocked after an attack, the attacker can register another domain name that was generated by the DGA. Recently malware that uses DGA are polymorphic, even when this malware is analyzed and the DGA is examined, the malware can generate different domain names dynamically, by using for example time information as a seed for that algorithm.

There is a way needed to defend against DGA-based malware. Current defense techniques against DGA-based malware is using string information of the generated domain names and analyzing these string information. The attackers avoid this kind of defense techniques by creating DGA that is generating domain names that are almost not distinguishable from normal domain names. To tackle this, there is a need for a new defense technique to differentiate the malicious based domain names from the unharmful ones. To solve this we will combine classification techniques and network traffic analysis.

Thus we can formulate our research question: **How to DGA-based malware using network traffic analysis and classifications.**

To steps that we have to take to answer this question:

1. Study about how domain generated algorithms work in well known malware and also look at the network patterns of these malware(especially DNS).
2. Use tools like “Cuckoo Sandbox” and “Wireshark” probably or any other tools in my disposal to get network packets .pcap from our malware samples.
3. Learn what kind of ways there are to analyze and detect DGA’s in a network packet .pcap. Study algorithms or Neural networks that could analyze and detect the malicious domain names that the DGA generated. Neural Networks like RNN + LTSM or RNN + Transformers to find out if the domain name that the DGA generated is malicious or not and/or using DNS traffic data to analyze it and find out any malicious content.
4. Create a “detector” or “analyzer” that can figure out if the DNS Communication or domain names that was generated in the .pcap file are malicious or not.
5. Use a lot of malware samples(for training data maybe) and unharmful normal programs that have network traffic(DNS traffic) to check for false positive and negatives.
6. Evaluate and discuss the results.
7. Conclude and give any suggestion for future research on this topic.