**Research Proposal  
Anti-Malware Technique**

**Research Proposal**

**Anti-malware Techniques**

**Purpose Statement:**

Malware is the biggest threat to internet users. A large number of malware attacks computers or mobiles connected to the internet (Zeltser, 2010). This malware is mostly developed and run by the criminal industry. They do this to get control over host computer.  There may be many reasons like ransom, tech support or installation of unwanted software for this attack. This malware has breached almost all the anti-malware/anti-virus and billions of internet users hosts are infected by them (Rieck, Trinius, Willems, & Holz, 2011).  One of the common methods of controlling host computer from a remote location is Remote Administrative Trojan/Tool (RAT). RAT is a software that allows remote control of host computer. Any device which is connected to TCP/IP or LAN may be controlled remotely (Hardy, 2012). The attacker may use different means like email attachment, chat software etc. to install this software on a host computer. Once installed, RAT uses sophisticated techniques to hide and stay in host computer or mobile for a longer period of time. This feature of hiding, staying, and stealing data for long periods is referred as Advanced Persistent Threats (APTs) (Kondalwar & Shelke, 2014). In spite of all these online threats, providing internet to smart devices/computers is no more a luxury but it is a necessity of present life.  IT department is the necessity of almost every industry (Lesakova, 2014), e-learning has enhanced the standard and flexibility of education. So, there is a need for some advancement in anti-malware technology.

**Statement of the Problem or Research Question(s):**

RQ1: Why existing anti-malware techniques are not 100 % successful in stopping RATs?

RQ2: How can existing anti-malware/RAT technology be improved?

**Significance of the Study:**

The effects and reasons of malware are already known (Mundie & Mcintire, 2013). Some work has already been done on behavior (Boileau, Gagnon, Poisson, Frenette, & Mejri, 2017), classification and analysis of malware (Sanabria, 2007). But less focus is made on the analysis of anti-malware techniques and reasons for low success rate. This study will focus on existing anti-malware techniques or software and try to analyze the reason for not getting 100 % success. Furthermore, some recommendations will be made at the end of this research for improvement in the development of anti-malware. This study will open new avenues of research for developing anti-malware techniques that have a higher success rate.

**List of References:**

Boileau, C., Gagnon, F., Poisson, J., Frenette, S., & Mejri, M. (2017). A Comparative Study of Android Malware Behavior in Different Contexts. *Universite Laval, Quebec, Canada*, 1–8. Retrieved from http://ieeexplore.ieee.org/document/7966340/

Hardy, S. (2012). *IEXPL0RE RAT*. Toronto, Canada.

Kondalwar, M. N., & Shelke, P. C. J. (2014). Remote Administrative Trojan / Tool ( RAT ). *International Journal of Computer Science and Mobile Computing*, *3*(3), 482–487.

Lesakova, L. (2014). SMALL AND MEDIUM ENTERPRISES IN THE NEW WORLD Of GLOBALIZATION. *Forum Scientiae Oeconomia*, *2*(3), 111–122.

Mundie, D. a., & Mcintire, D. M. (2013). *The MAL: A Malware Analysis Lexicon*. *Software Engineering Institute*. https://doi.org/10.1109/ARES.2013.73

Rieck, K., Trinius, P., Willems, C., & Holz, T. (2011). Automatic Analysis of Malware Behavior Using Machine Learning. *Journal of Computer Security*, *19*(4), 639–668. https://doi.org/10.3233/JCS-2010-0410

Sanabria, A. (2007). Malware Analysis: Environment Design and Architecture. *SANS Institute: InfoSec Reading Room*, *1*, 1–60.

“Understand the Different Malware Types.” *Microsoft*, 9 Feb. 2018, www.microsoft.com/en-us/wdsi/threats.

Zeltser, L. (2010). *Introduction To Malware Analysis*.