PROFILING NATIONAL STATE ACTORS AND ANALYSIS OF TACTICS, TECHNIQUES AND PROCEDURES BASED ON MITRE ADVERSARIAL TACTICS, TECHNIQUESAND COMMON KNOWLEDGE (ATT&CK) FRAMEWORK

By

Syed Hassan Murad Ali Shah

00000327868

A thesis submitted to the National University of Sciences and Technology,

Islamabad, in partial fulfillment of the requirements for the degree of

Masters of Science

in Information

Security

Thesis Supervisor: Brig Imran Rashid, Phd

Co-Supervisor: Dr. Haider Abbass, Phd

Military College of Signals

National University of Sciences &

Technology(NUST) Islamabad,Pakistan

THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS Thesis written by **Mr.Syed Hassan Murad Ali Shah** Registration No.**00000327868**, of **Military College of Signals** hasbeenvetted by undersigned, found complete in all respects as per NUST Statutes/ Regulations/ MS Policy, is free of plagiarism, errors, and mistakes, and is accepted as partialfulfillment for the award of MS degree. It is further certified that necessary amendments as pointed out by GEC members and foreign/ local evaluators of the scholar have also been incorporated in the saidthesis.

Signature:_____

Name ofSupervisor:**Brig Imran Rashid, Phd**

Date:_____

Signature:_____

Date:_____

Signature:_____

Date:_____

Author's Declaration

I certify that this research work titled "**Profiling National State Actors And Analysis Of Tactics, Techniques And Procedures Based On Mitre Adversarial Tactics, Techniques, And Common Knowledge (ATT&Ck) Framework**" is my work. No portion of this work presented in this dissertation has been submitted in support of another award or qualification either at this institution or elsewhere. The material that has been used from other sources has been properly acknowledged/referred to.

_____

Signature of Student

Syed Hassan Murad

00000327868

Plagiarism Undertaking

Isolemnlydeclarethatthe researchworkpresentedinthethesistitled"**Profiling National State Actors And Analysis Of Tactics, Techniques And Procedures Based On Mitre Adversarial Tactics, Techniques, And Common Knowledge (ATT&CK) Framework**" is solely my research work with no significant contribution from any other person. Small contribution/ help wherever taken has been duly acknowledged and that complete thesis has been written by me.

I understand the zero-tolerance policy of the HEC and Military College of Signals, NUST towards plagiarism. Therefore, I as an author of the above-titled thesis declare that no portion of my thesis has been plagiarized and any material used as reference is properly referred to/cited.

IundertakethatifIamfoundguiltyofanyformalplagiarismintheabove-titledthesiseven after awarding of MS degree, the University reserves the right to withdraw/revoke my MS degree and that HEC and the University have the right to publish my name on the HEC/Universitywebsiteonwhichnamesofstudentsareplacedwhosubmittedplagiarized thesis.

Student/AuthorSignature:_____

Name:_____

DEDICATION

This thesis is dedicated to

MY FAMILY

for their love, endless support and encouragement

ACKNOWLEDGEMENTS

I am grateful to Allah Almighty for giving me strength to keep going on with this thesis, irrespective of many challenges and troubles. All praises for HIM and HIM alone.

I am very grateful to my Project Supervisor Brig Imran Rashid,Phd, Co-Supervisor DrHaiderAbbass and GEC members who supervised the thesis / research in a very encouraging and helpful manner. They always guided me with their profound and valuable support that have helped me in achieving my research aims.

I would like to extend my feelings of gratitude towards my Parents for encouraging me to take on this endeavor to complete this degree. I would like to express my appreciation to all the people who have provided valuable support to my study and whose names I couldn't bring to memory.

ABSTRACT

Within our generation we have seen that the nature of threats has slowly changed. They have now evolved to threats without borders and that is an alarming issue. With this work we have tried to solve a problem of identifying those threats for ourselves. The problem that our organizations, both civil and military face is not just the threats that exist but also their motives. The reason for making Mitre ATT&CK framework the core of this research was that it offers an advanced approach as compared to Cyber Kill Chain (CKC). That approach goes through a very thoroughly and systematically created way of not just identifying a threat but also tracing all its steps. With regards to Mitre Framework within Pakistan there is little to no research done and hence I want this to be a starting point for students to add to the work of profiling threats that exist. The reason for choosing profiling is because the best way to stop an intruder is to know where they'll come from and how to put a stop there. That question is only answered in Mitre ATT&CK framework. With my research I have profiled approximately 800 entities with different Alias and signatures from around the world. The future of this research can be brought to fruition by continuously adding to it and utilizing the Common Knowledge platform of OpenCTI. That platform can be used to our advantage and identify and upgrade the adding amount of threats on daily basis. In short this research is not just a platform for identifying threats but also helping organizations to quickly identify one and save time which would in-turn save the precious data very dear to every entity whether individual or national.

Keywords: Profiling, State Actors, Mitre ATT&CK Framework.

TABLE OF CONTENTS

Contents

LIST OF FIGURES