

University of Reading

Department of Computer Science

“Investigating the Parallels between using a RAT-style software for malicious Intent and Virtuous Purposes”.

Daniel Broomhead

*Supervisor:* Dr Mohammed Al-Khafajiy

A report submitted in partial fulfilment of the requirements of the University of Reading for the degree of

Bachelor of Science in *Computer Science*

April 29, 2021

Declaration

I, Daniel Broomhead, of the Department of Computer Science, University of Reading, confirm that all the sentences, figures, tables, equations, code snippets, artworks, and illustrations in this report are original and have not been taken from any other person’s work, except where the works of others have been explicitly acknowledged, quoted, and referenced. I understand that if failing to do so will be considered a case of plagiarism. Plagiarism is a form of academic misconduct and will be penalised accordingly. I give consent to a copy of my report being shared with future students as an exemplar. I give consent for my work to be made available more widely to members of UoR and public with interest in teaching, learning and research.

Daniel Broomhead April 29, 2021

Word Count:

Prerequisites: 591 + 711 = 1302

Main Report: 18666 = 19968

References: 1091 = 21059

Appendix (including PID & Code): 5632 = **26691**

Total:

Abstract

**The constant desire for humans to adapt and evolve, ultimately performing more efficiently has historically been a major driving force for the advancements in technology, humans no longer have the requirement to have physical access to a device, in order to perform maintenance or tasks which would have required this.**

**Remote Access is not a new concept. Since the Beginning of the internet and the ability of connecting devices together, the idea of controlling and accessing a device from another device has been extremely prevalent. The methods of doing this, the protocols used, and interfaces used have been changed, updated, and refreshed countless times, however the origins of the idea date back decades.**

**In fact, their uses track back to the early days of the internet, and the mid-late 1990’s where tech-savvy kids would commonly use them to scare and prank their friends by controlling their PC’s remotely. This could be simple annoyances like ejecting the CD from the CD tray, swapping mouse buttons, or changing the desktop colours. To an unwitting user, it would appear as if a ghost was in control of their device. This is widely accepted as the era beholding the birth of the Remote Access Tools.**

Keywords: ... RAT, Remote Access Tool, Remote Administration Trojan, UoRAT

Acknowledgements:

**I would like to take the opportunity to express my sincere appreciation to the people who were involved in my journey through this project and my time at the University of Reading. First, I would like to extend my thanks towards my project supervisor, Dr. Mohammed Al-Khafajiy for his help and guidance. I would also like to express my gratitude towards Dr. Julian Kunkel, who continuously supported me throughout my time as University, as both an Academic Mentor and a member of staff who always strived to make sure the students were challenged and engaged.**

**I would like to express a deep thanks to my colleagues, friends and family who have constantly supported me and pushed me to be the best that I could be, both academically and generally. Their continuous motivation and perseverance, alongside the examples that they have set throughout has been paramount to my achievements at University. A special mention is dedicated to Amadeusz Włodarczyk, Edwin Park, Joseph Mckeown and Savva Podkopov, who throughout University have spent countless hours and late nights beside me working on each coursework to ensure the best outcomes.**

# Contents

1. Introduction 1
   1. ... . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 1
      1. .. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 1
   2. Summary of contributions and achievements . . . . . . . . . . . . . . . . . . 1
   3. Organization of the Report . . . . . . . . . . . . . . . . . . . . . . . . . . . 1
2. Literature Review 2
   1. ... . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 2
   2. ... . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 2
      1. ... . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 2
   3. Summary . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 2
3. Methodology 3
   1. ... . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 3
   2. Summary . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 3
4. Results 4
   1. ... . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4
   2. ... . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4
   3. Summary . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4
5. Discussion and Analysis 5
   1. .. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 5
   2. Summary . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 5
6. Conclusions and Future Work 6
   1. Conclusions . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 6
   2. Future Work . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 6
7. Reflection 7

Appendices 9

1. An Appendix ..... 9
2. An Appendix ... 10

Chapter 1

# Introduction

...

1.1 ...

....

1.1.1 ..

..

1.2 Summary of contributions and achievements

...

1.3 Organization of the Report

..

Chapter 2

# Literature Review

...

2.1 ...

....

2.2 ...

...

2.2.1 ...

2.3 Summary

...

Chapter 3

# Methodology

...

3.1 ...

...

3.2 Summary

Chapter 4

# Results

..

4.1 ...

..

4.2 ...

...

4.3 Summary

Chapter 5

# Discussion and Analysis

...

5.1 ..

5.2 Summary

Chapter 6

# Conclusions and Future Work

...

6.1 Conclusions

...

6.2 Future Work

...

Chapter 7

Reflection

...

## **References**

[1]"Stone Tools | The Smithsonian Institution's Human Origins Program", *Humanorigins.si.edu*, 2020. [Online]. Available: https://humanorigins.si.edu/evidence/behavior/stone-tools#:~:text=Early%20Stone%20Age%20Tools,-The%20earliest%20stone&text=The%20Early%20Stone%20Age%20began,and%20other%20large%20cutting%20tools. [Accessed: 29- Apr- 2021].

[2]A. Safe, "How Does a Master Key Work?", *Aim Lock and Safe*, 2013. [Online]. Available: https://www.aimlockandsafe.ca/blog/how-does-a-master-key-work/. [Accessed: 29- Apr- 2021].

[3]"What Is a Skeleton Key? | Antique Skeleton Keys | Anderson Lock", *Anderson Lock*, 2021. [Online]. Available: https://www.andersonlock.com/blog/collecting-antique-keys/. [Accessed: 29- Apr- 2021].

[4]D. Peterson, *2017 Maps of Meaning 02: Marionettes & Individuals (Part 1)*. 2017.

[5]D. Peterson, "Jordan Peterson | Maps of Meaning", *Jordan Peterson*, 2018. [Online]. Available: https://www.jordanbpeterson.com/maps-of-meaning/. [Accessed: 29- Apr- 2021].

[6]W. Churchill, "The long arm of Destiny", Harvard, Sept 1943.

[7]S. Raimi, *Spider-Man*. Los Angeles: Columbia Pictures, 2002.

[8]S. O'Grady, "The RedMonk Programming Language Rankings: January 2021", *tecosystems*, 2021. [Online]. Available: https://redmonk.com/sogrady/2021/03/01/language-rankings-1-21/. [Accessed: 29- Apr- 2021].

[9]"Infographic: Python Remains Most Popular Programming Language", *Statista Infographics*, 2020. [Online]. Available: https://www.statista.com/chart/21017/most-popular-programming-languages/. [Accessed: 29- Apr- 2021].

[10]"What Is a Socket? (The Java™ Tutorials > Custom Networking > All About Sockets)", *Docs.oracle.com*, 1995. [Online]. Available: https://docs.oracle.com/javase/tutorial/networking/sockets/definition.html#:~:text=Definition%3A,address%20and%20a%20port%20number. [Accessed: 29- Apr- 2021].

[11]K. Thompson, "Basics of the Unix Philosophy", *Catb.org*, 1974. [Online]. Available: http://www.catb.org/esr/writings/taoup/html/ch01s06.html. [Accessed: 29- Apr- 2021].

[12]J. Santos, "XP, FDD, DSDM, and Crystal Methods of Agile Development", *Project-Management.com*, 2018. [Online]. Available: https://project-management.com/xp-fdd-dsdm-and-crystal-methods-of-agile-development/. [Accessed: 29- Apr- 2021].

[13]"Leetspeak: The History of Hacker Culture's Native Tongue | Alpine Security", *Alpine Security*, 2021. [Online]. Available: https://alpinesecurity.com/blog/leetspeak-the-history-of-hacker-culture/. [Accessed: 29- Apr- 2021].

[14]"PEP 636 -- Structural Pattern Matching: Tutorial", *Python.org*, 2020. [Online]. Available: https://www.python.org/dev/peps/pep-0636/. [Accessed: 29- Apr- 2021].

[15]"PEP 635 -- Structural Pattern Matching: Motivation and Rationale", *Python.org*, 2020. [Online]. Available: https://www.python.org/dev/peps/pep-0635/. [Accessed: 29- Apr- 2021].

## **References**

[16]"PEP 634 -- Structural Pattern Matching: Specification", *Python.org*, 2021. [Online]. Available: https://www.python.org/dev/peps/pep-0634/. [Accessed: 29- Apr- 2021].

[17]"PEP 324 -- subprocess - New process module", *Python.org*, 2021. [Online]. Available: https://www.python.org/dev/peps/pep-0324/. [Accessed: 29- Apr- 2021].

[18]"subprocess — Subprocess management — Python 3.9.4 documentation", *Docs.python.org*, 2021. [Online]. Available: https://docs.python.org/3/library/subprocess.html. [Accessed: 29- Apr- 2021].

[19]D. Goodin, "How Soviets used IBM Selectric keyloggers to spy on US diplomats", *Ars Technica*, 2015. [Online]. Available: https://arstechnica.com/information-technology/2015/10/how-soviets-used-ibm-selectric-keyloggers-to-spy-on-us-diplomats/. [Accessed: 29- Apr- 2021].

[20]"shutdown", *Docs.microsoft.com*, 2017. [Online]. Available: https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/shutdown. [Accessed: 29- Apr- 2021].

[21]"pyscreenshot", *PyPI*, 2021. [Online]. Available: https://pypi.org/project/pyscreenshot/. [Accessed: 29- Apr- 2021].

[22]"opencv-python", *PyPI*, 2021. [Online]. Available: https://pypi.org/project/opencv-python/. [Accessed: 29- Apr- 2021].

[23]"PyAutoGUI", *PyPI*, 2021. [Online]. Available: https://pypi.org/project/PyAutoGUI/. [Accessed: 29- Apr- 2021].

[24]"Pillow", *PyPI*, 2021. [Online]. Available: https://pypi.org/project/Pillow/. [Accessed: 29- Apr- 2021].

[25]"mss", *PyPI*, 2021. [Online]. Available: https://pypi.org/project/mss/. [Accessed: 29- Apr- 2021].

[26]B. Vollebregt, "How To Take A Screenshot In Python Using MSS", *Nitratine.net*, 2020. [Online]. Available: https://nitratine.net/blog/post/how-to-take-a-screenshot-in-python-using-mss/. [Accessed: 29- Apr- 2021].

[27]"Examples — Python MSS latest documentation", *Python-mss.readthedocs.io*, 2020. [Online]. Available: https://python-mss.readthedocs.io/examples.html. [Accessed: 29- Apr- 2021].

[28]D. Brunner, "Frame Rate: A Beginner's Guide | TechSmith", *Welcome to the TechSmith Blog*, 2017. [Online]. Available: https://www.techsmith.com/blog/frame-rate-beginners-guide/. [Accessed: 29- Apr- 2021].

[29]"Usage — Python MSS latest documentation", *Python-mss.readthedocs.io*, 2020. [Online]. Available: https://python-mss.readthedocs.io/usage.html. [Accessed: 29- Apr- 2021].

[30]S. Jansen, "STAR WARS ASCIIMATION - Main Page", *Asciimation.co.nz*, 2021. [Online]. Available: https://asciimation.co.nz/index.php. [Accessed: 29- Apr- 2021].

## **References**

[31]"FICS Quick Guide", *Freechess.org*, 1998. [Online]. Available: https://www.freechess.org/QuickGuide/. [Accessed: 29- Apr- 2021].

[32]"About Us | Weather Underground", *Wunderground.com*, 2021. [Online]. Available: https://www.wunderground.com/about/our-company. [Accessed: 29- Apr- 2021].

[33]"State of the Internet: Fewer Attacks Than Previous Quarter - The Akamai Blog", *Blogs.akamai.com*, 2014. [Online]. Available: https://blogs.akamai.com/2014/06/state-of-the-internet-fewer-attacks-than-previous-quarter.html. [Accessed: 29- Apr- 2021].

[34]"state-of-the-internet/akamai-q4-2010-state-of-the-internet-connectivity-report.pdf", *Akamai.com*, 2010. [Online]. Available: https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-q4-2010-state-of-the-internet-connectivity-report.pdf. [Accessed: 29- Apr- 2021].

[35]"state-of-the-internet/akamai-q2-2010-state-of-the-internet-connectivity-report.pdf", *Akamai.com*, 2010. [Online]. Available: https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-q2-2010-state-of-the-internet-connectivity-report.pdf. [Accessed: 29- Apr- 2021].

[36]"state-of-the-internet/akamai-q3-2010-state-of-the-internet-connectivity-report.pdf", *Akamai.com*, 2010. [Online]. Available: https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-q3-2010-state-of-the-internet-connectivity-report.pdf. [Accessed: 29- Apr- 2021].

[37]"state-of-the-internet/akamai-q1-2010-state-of-the-internet-connectivity-report.pdf", *Akamai.com*, 2010. [Online]. Available: https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-q1-2010-state-of-the-internet-connectivity-report.pdf. [Accessed: 29- Apr- 2021].

[38]N. Mott, "Report: Hacker Publishes Credentials for 500,000 Telnet Devices | Tom's Hardware", *Tomshardware.com*, 2020. [Online]. Available: https://www.tomshardware.com/news/report-hacker-publishes-credentials-for-500000-telnet-devices. [Accessed: 29- Apr- 2021].

[39]C. Cimpanu, "Hacker leaks passwords for more than 500,000 servers, routers, and IoT devices | ZDNet", *ZDNet*, 2019. [Online]. Available: https://www.zdnet.com/article/hacker-leaks-passwords-for-more-than-500000-servers-routers-and-iot-devices/. [Accessed: 29- Apr- 2021].

[40]C. Cimpanu, "Someone Published a List of Telnet Credentials for Thousands of IoT Devices", *BleepingComputer*, 2017. [Online]. Available: https://www.bleepingcomputer.com/news/security/someone-published-a-list-of-telnet-credentials-for-thousands-of-iot-devices/. [Accessed: 29- Apr- 2021].

[41]T. Seals, "Million+ IoT Radios Open to Hijack via Telnet Backdoor", *Threatpost.com*, 2019. [Online]. Available: https://threatpost.com/million-iot-radios-hijack-telnet-backdoor/148123/. [Accessed: 29- Apr- 2021].

[42]M. Alvarez, "Consequences of IoT and Telnet: Foresight Is Better Than Hindsight", *Security Intelligence*, 2016. [Online]. Available: https://securityintelligence.com/consequences-of-iot-and-telnet-foresight-is-better-than-hindsight/. [Accessed: 29- Apr- 2021].

[43]"email.mime: Creating email and MIME objects from scratch — Python 3.9.4 documentation", *Docs.python.org*, 2021. [Online]. Available: https://docs.python.org/3/library/email.mime.html. [Accessed: 29- Apr- 2021].

[44]"Platform Module in Python - GeeksforGeeks", *GeeksforGeeks*, 2020. [Online]. Available: https://www.geeksforgeeks.org/platform-module-in-python/#:~:text=Python%20defines%20an%20in%2Dbuilt,program%20is%20being%20currently%20executed. [Accessed: 29- Apr- 2021].

[45]"How to Install Python Packages using a Script", *ActiveState*, 2021. [Online]. Available: https://www.activestate.com/resources/quick-reads/how-to-install-python-packages-using-a-script/. [Accessed: 29- Apr- 2021].

Appendix A

An Appendix .....

...

Appendix B An Appendix ...

...