# Visualizing Malware Propagation Across Local Area Networks

Jacob J Williams

## Abstract

## Introduction

Malware is perhaps one of the greatest threats in modern day IT, it is constantly evolving both terms of who it targets and what it exploits. Due to the evolutionary nature of malware modern security has turned into a cat and mouse game, security analysts and malware writers always vying to overtake the other by finding new ways to protect or exploit systems. Unfortunately it is common in the industry for the malware writers always to be numerous steps ahead, with those who work in security being forced to operate reactively to malware, this is why the security industry needs more who are willing to study malware in order to prevent it.

How malware propagates is key to understand how malware operates, external propagation; that being how malware bridges the air gap between networks is commonly studied and is fairly established in various forms of study, mathematically and visually. How malware propagates within a local area network however is studied rather one sidedly, leaning towards the mathematical side. These studies are extremely comprehensive and explore numerous methodologies of formulating how malware propagates, but it requires some complex knowledge and understanding of mathematical models and theories and as a result could be seen as being rather unfriendly to those wishing to involve themselves with Cyber Security from other backgrounds. Therefore the goal of this study to to attempt to visualise malware propagation using variables and characteristics from machines on local area networks and produce a more easily interpretable way of showing the nature of propagation.

### 1.1 Aims and Objectives

1. To create a visualization tool for examining the propagation of threats across a local area network with an initial focus on the subset of Ransomware and then proceeding to the superset of malware afterwards.
2. To create clear and interpretable visualisations of propagations.
   1. To inform other researchers of the details of the propagation in order to assist in the further development of anti-malware capabilities.
   2. To inform those in positions whose decisions can affect the security of a network, and where they should be deploying network security features.
   3. To aid students in the study of malware behaviour and its impact across networks.
3. To identify key characteristics of malware propagation that can be used in the response to an attack.

The second aim is the crux of this research, as aforementioned there already exist numerous studies into malware propagation but in the form of mathematical formulas and graphs that are only interpretable by those with prior experience or study in the field of Cyber Security or mathematics. Therefore this research hope to contribute to the study of malware prevention by creating resources for those who either just beginning their studies or those less knowledgeable in the field of Security and wish to utilise the results of such studies in configuring their network security.

## Related Literature

## Methodology

### 3.1 Timeline

### 3.2 Ethics