Jacob Williams University of the West of England 15008632

Visualising Ransomware Propagation Across Local Area Networks

Abstract

Ransomware has grown into one of the biggest threats to businesses and IT infrastructure in recent years. The attack method has always existed, but the recent trend in the increase of the value of data and the requirement for availability has lent a hand in magnifying the impact of a ransomware attack. Such attacks can be absolutely devastating to businesses, the WannaCry NHS attack rendered multiple hospitals across the UK defective for numerous weeks and it wasn't the intended target. Current research into the field has explored methods of preventing ransomware attacks; the research in this paper intends to study and visualize how ransomware propagates across an already compromised network in order to better inform those who create or install security features on larger networks.

Aims

The aims for this project are as follows:

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 after.
2. To create clear and interpretable visualisations of propagations.
    a. To inform other researchers on the details of the propagations in order to assist in the further development of anti-ransomware or malware capabilities.
    b. To inform those in positions whose decisions can affect the security of a network, and where they should be deploying network security features (Network Engineers, business owners).
    c. To aid students in the study of Ransomware behaviour and its impact across networks.
3. To identify key characteristics of Ransomware propagation that can be used in the response to a Ransomware attack.

The second aim is the crux of this research, there already exist numerous studies into the area of Malware propagation but often the papers present the findings 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 Computer Science. Therefore, this research hopes to contribute to the Ransomware prevention effort by bringing knowledge of its propagation to those who are 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.

Research

Below are a sample of the research papers being used to assist in this project:

- Yu, S.Y., Gu, G.G., Barnawi, A.B., Guo, S.G., and Stojmenovic, I.S. (2015) Malware Propagation in Large-scale Networks. *Ieee Transactions on Knowledge and Data Engineering* [online]. 27 (1), pp. 170-179. [Accessed 30 January 2020].

- Gove, R. and Deason, L. (2018) Visualizing Automatically Detected Periodic Network Activity. Available from: osf.io/xpwfedoi:10.31219/osf.io/xpwfe [Accessed 27 January 2020].

- Zhuo, W.Z. and Nadjin, Y.N. (2012) Malwarevis: Entity-based Visualization of Malware Network Traces. *Vizsec* [online]. 12, pp. 41-47. Available from: https://doi.org/10.1145/2379690.2379696 [Accessed 29 January 2020].
- Mills, A.M., Legg, P.L. and Spyridopoulos, T.S. (2019) Efficient and Interpretable Real-time Malware Detection Using Random-forest. *Ieee* [online]. Available from: doi.org/10.1109/CyberSA.2019.8899533 [Accessed 12 December 2019].