**NCSC Summer Internship Scheme 2020 - Expression of Interest**

**Student Name:** Jacob Williams

**Project Title:** Analysis and Visualisation of Ransomware and Malicious Network Propagation

**Project Supervisor:** Dr Phil Legg

**Institution:** University of the West of England

**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 despite not being a targeted attack. Current research into the field has explored methods of preventing ransomware attacks; the research in this paper extends on this notion to analyse, and visualise, how both malware and malicious users may propagate across a network to better inform security analysts and to deploy appropriate responses to attacks.

**Aims**

The aims for this project are as follows:

1. To develop a dynamic network generation environment for the purpose of conducting experimentation into malware and malicious user network propagation.
2. 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. The tools should create clear and interpretable visualisations of propagations:
   1. To inform other researchers on the details of the propagations in order to assist in the further development of anti-ransomware or 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 (Network Engineers, business owners).
   3. 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, or the presence of malicious user network propagation. Responses provided by the dynamic network environment could then include network reconfiguration, device isolation, or deployment of a deception network.

**References**

* 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].