Department	School of Computing
Supervisors	Rich Macfarlane, Dr Gordon Russell
Project Title	Behavioural Analysis for Ransomware Detection

PROJECT DESCRIPTION

Edinburgh Napier University's Cyber Security and Forensics Research Group focuses on applied research in core areas of threat analysis and detection, digital forensic triage, trust, identity and cryptography, and has had successful real-world impact with several spin-out companies, including in the area of Ransomware.

Ransomware is a type of malware used in extortion-based attacks, which typically lock and steal user data, and then demand payment from the victim in return for their safe files and data. Over the last few years ransomware has become a very large threat to corporate as well as personal data, and has seen rapidly evolving tactics and techniques to evade detection and mitigation.

This project aims to extend current research work around the analysis and detection of ransomware attacks, particularly focused on behavioural analysis early in the kill chain. A focus on pre-destructive activity detection and dynamic behaviour analysis, including methods to analyse features such as API calls and file interactions. The scope of the work and focus of the individual project can be, to some extent, driven by the individual student. The work will be carried out within a small team of researchers here at Edinburgh Napier University working at the forefront of Ransomware research, including various research projects the areas of ransomware analysis, detection and mitigation.

A short research proposal of around 1,000 words outlining the specific project, is expected as part of the application. The project will be supervised by Associate Professor Rich Macfarlane (r.macfarlane@napier.ac.uk) and others from the team. Interested students are encouraged to contact Rich by email to discuss the proposal.

Academic qualifications

A first degree (at least a 2.1) or MSc ideally in Computer Science-related area with a good fundamental knowledge of computer science and ideally cyber security.

English language requirement

IELTS score must be at least 6.5 (with not less than 6.0 in each of the four components). Other, equivalent qualifications will be accepted. Full details of the University's policy are available online.

Essential attributes:

- Strong focus on applied cyber security concepts, such as the attack kill chain, classification of threat information, offensive security.
- Good written and oral communication skills.
- Strong motivation, with evidence of independent research skills.
- Good organisation and time management skills.

Desirable attributes:

- Research skills.
- Programming and software testing.
- Offensive security, and malware analysis ideally.

Indicative Bibliography	McIntosh, T., Kayes, A. S. M., Chen, Y. P. P., Ng, A., & Watters, P. (2021). Ransomware mitigation in the modern era: A comprehensive review, research challenges, and future directions. *ACM Computing Surveys (CSUR)*, *54*(9), 1-36. Sihwail, R., Omar, K., & Ariffin, K. A. Z. (2018). A survey on malware analysis techniques: Static, dynamic, hybrid and memory analysis. *International Journal on Advanced Science, Engineering and Information Technology*, *8*(4-2), 1662. N. Hampton, Z. Baig, and S. Zeadally, "Ransomware behavioural analysis on windows platforms," Journal of information security and applications, vol. 40, pp. 44–51, 2018. Davies, S. R., Macfarlane, R., & Buchanan, W. J. (2020). Evaluation of live forensic techniques in ransomware attack mitigation. Forensic Science International: Digital Investigation, 33, 300979.
Enquiries	For informal enquiries about this PhD project, please contact r.macfarlane@napier.ac.uk
Web page	https://www.napier.ac.uk/research-and-innovation/research-degrees/application-process