

Academics from Napier take on the hackers

Edinburgh Napier University cyber security experts have created a new data set which will support cutting-edge research into detecting ransomware.

This is the malware which can be used to attack computer systems, allowing hackers to demand a ransom for its removal. .

Newly created NapierOne can now use new methods and updated data sets, and is allowing this to be used as open access. It is hoped this will speed up the research into ransomware and get ahead of the hackers.

One of the data sets which is publicly available is Govdocs1 which is now more than ten years old, and there are doubts about how effective it is. A PhD student at Edinburgh Napier has worked with university academics to write a new paper about Digital Investigation which details their research creating a data set of more than 50,000 unique files.

PhD candidate Simon Davies said: "It is hoped that the adoption of the NapierOne data set into the implementation, development and testing lifecycles of new ransomware detection techniques will streamline and accelerate the development of

more robust and effective detection techniques, allowing independent researchers to reproduce and validate proposed detection methods quickly.”



Edinburgh Napier’s Cyber Academy, based within the School of Computing, has opened a new, state of the art security operations centre at our Merchiston campus, in collaboration with IT security company Satisnet.
Professor Bill Buchanan portrait.



Portrait of Rich MacFarlane



Associate Professor Rich Macfarlane
Associate Professor Rich Macfarlane said: “Ransomware has been around for many years – encrypting and deleting users’ files

and demanding a ransom from the victim. It has become increasingly common and its sophistication has increased significantly, leading to it currently being the biggest cyber security problem globally.

“This work aims to provide a research data set allowing scientific rigour in research towards fighting the ransomware problem. The data set has been created and successfully used in our ransomware detection research. Containing over half a million unique files representing real world file types, it is broad and diverse enough to be used in a range of cyber security and forensic research areas.

“We hope the data set will have the same global research impact as the Govdocs1 work.”

Professor Bill Buchanan said: “There are few areas of cyber security that need more of a scientific base than in digital investigations, and thus there exists a need to make sure investigators have appropriate tools that have been verified and properly evaluated. This data set provides a foundation for researchers to prove their new methods, and thus further support innovation in the area.

“The UK is becoming an international leader in the field of safe technology – which involves the development of tools to support digital investigations and threat detection – and this research showcases the development of a strong scientific base.”