Greater Manchester | Greater Security | Greater Business
Cyber Foundry

Security News of the Week

by Thomas Martin, Manchester Metropolitan University, Senior Lecturer

Tuesday 20th July 2021

Pegasus: Spyware sold to governments 'targets activists'

Reports are surfacing about a leaked list of 50,000 phone numbers of interest to clients of the company NSO Group. NSO Group are believed to provide malware (named Pegasus) to nation states (including authoritarian governments) to spy on individuals. Their malware is believed to grant full access to all content on any device infected. While NSO Group claims their malware is only intended for use against criminals and terrorists, the leaked list includes journalists, business executives, activists, politicians, and heads of state. It has not been confirmed how many of the 50,000 were infected by Pegasus. Read more>

Northern's ticket machines hit by ransomware cyber attack

Northern Rail have been hit by a ransomware attack. Their newly installed touch-screen units are offline due to the impact on the supporting servers. The supplier, Flowbird, has given assurances that customer and payment data has not been comprised. Web and app purchasing does not appear to have been impacted.
Read more>

Saudi Aramco data breach sees 1 TB stolen data for sale

One of the largest petroleum and natural gas companies in the world are being extorted over a data breach. The hacking group known as "ZeroX" is offering 1TB of data from Saudi Aramco at a cost of $5 million (but they are willing to negotiate). Saudi Aramco divulged that the data breach was due to a third-party contractor and that no encryption of their systems took place (i.e., not a ransomware attack). The data is alleged to include employee information, project specifications, internal analysis reports, and networking information. Some redacted samples of the data have been released, and a 1GB sample can be purchased for $2,000 in Monero (XMR). ZeroX did attempt to contact Aramco but after not receiving a response did not make any attempt to directly extort them. Read more>

US and allies officially accuse China of Microsoft Exchange attacks

The United States is officially accusing China of orchestrating the recent hacking campaign against Microsoft. The White House has said that "with a high degree of confidence" they believe that the Chinese Ministry of State Security (MSS) was behind the exploitation of the ProxyLogon zero-day vulnerability. The attack targeted over a quarter of a million Exchange servers and impacted tens of thousands of organisations. Several of the US's allies have also backed the statement, including the UK's own GCHQ. Read more>

European Union
European Regional Development Fund
Manchester Metropolitan University
MANCHESTER 1824 The University of Manchester
University of Salford MANCHESTER
Lancaster University