Greater Manchester | Greater Security | Greater Business

Cyber Foundry

Security News of the Week

by Thomas Martin, Manchester Metropolitan University, Senior Lecturer

Monday 21st September 2020

Maze attackers adopt Ragnar Locker virtual machine technique

Ransomware criminals are having to take ever more elaborate steps to avoid detection. The perpetrators of the Maze ransomware attacks deployed a 2 GB Windows 7 virtual machine on the victims' machines in order to hide the existence and operation of a 494 KB binary This builds on the Ragnar Locker approach that used a smaller Windows XP VM. Read here>

Tor ODay: Fnding IP Addresses

The Tor network is designed to provide strong anonymity for users and hidden services. Assumptions are made about the capabilities of any adversaries looking to identify who is doing what. This blog posts talks about how there are entities out there that have much greater capabilities than allowed for (observation of global traffic and the ability to DDoS nodes to take them offline) and what it means for the actual privacy Tor offers: Read here>

'German Hospital Hacked, Patient Taken to Another City Dies

A tragic story in Germany of a cyber-attack leading to the death of a woman seeking treatment. The Duesseldorf University Hospital suffered from a ransomware attack, and as a result had to direct emergency patients elsewhere. After travelling another 32 kilometres to the next nearest hospital, doctors were unable to save the patient's life. The attack was apparently targeted at the affiliated Heinrich Heine University. When the attackers were notified that it was the hospital that was affected, the ceased the attack and provided the decryption keys. Police are investigating it as possible negligent manslaughter. Read here>

Twitter beefs up security for US election candidates

Twitter are increasing the security of high-profile US politicians in the run up the US election. New requirements include in-app notifications of changes, password reset protection, and strong passwords. Two-factor authentication is recommended, not required. Read here>

Targeted ransomware attacks on the UK education sector by cyber criminals

The NCSC (National Cyber Security Centre) has issued an alert on the increase of ransomware attacks targeting the UK education sector. Read here>

In recent weeks, both Newcastle and Northumbria Universities have admitted to falling victim to attacks. The NCSC recommend frequent patching, multi-factor. Read here>

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