Greater Manchester | Greater Security | Greater Business

Cyber Foundry

Security News of the Week

by Thomas Martin, Manchester Metropolitan University, Senior Lecturer

Monday 1st February 2021

WORLD'S MOST DANGEROUS MALWARE EMOTET DISRUPTED THROUGH GLOBAL ACTION

Europol have announced the successful takedown of the Emotet botnet. Emotet has been regarded as one of the most serous malware threats of recent times. The primary propagation means is via macro-enabled Word documents spread by email. They have used various lures to get users to open the documents (and enable macros), including invoices, shipping notices, and information about COVID-19. Europol, working with several national law enforcement agencies, were able to infiltrate several of the hundreds of servers responsible for maintaining the Emotet botnet and take it down from within. Infected machines have been redirected to law enforcement-controlled infrastructure for remediation. Read more>

Fonix ransomware shuts down and releases master decryption key

The Fonix Ransomware operators have announced that they are shutting down their activities. They have released a master decryption key and decryption software. The announcement suggests the operators want to turn over a new leaf, but also mention that it was not a unanimous decision (hinting there may be a future splinter group). The key has been confirmed to work, but only on some versions of the Fonix ransomware, and the provided software is unreliable. A fully operational decryptor is expected to soon be provided by Anti-Malware provider Emisosft. Read more>

'I was scammed out of £17,000 on Instagram'

Reports of frauds on social media have increased under lockdown. The average number of Instagram have gone up by more than 50%, according to the UK Police's Action Fraud. The BBC are reporting on one case where the victim lost £17,000. He fol
lowed an account on Instagram of someone claiming to have got rich quick through foreign exchange trading. He was encouraged to setup a trading account on the Infinox platform and give the fraudster control over trading. After some brief positive trading, the funds were entirely withdrawn. Facebook say they are actively taking down inauthentic accounts all the time. Investors are advised to only deal with financial firms that are authorised by the FCA. Read more>

Ghost hack – criminals use deceased employee's account to wreak havoc

There is a report of a ransomware attack on a company which had been infiltrated for a month. Sophos describe some of the details of the attack, which was unusual as the attackers had initially obtained access through a deceased former employee. Ex-employee accounts being abused is not uncommon but is more typically a case of a disgruntled former employee wishing to cause sabotage. In this case, the account of the deceased sysadmin needed to stay active because the credentials were used in various internal services. Read more>

Cybersecurity tips for university students

Sophos have released a list of five cybersecurity tips for University students (but the list is suitable for any general audience). Read more>

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