Greater Manchester | Greater Security | Greater Business

Cyber Foundry

Security News of the Week

by Thomas Martin, Manchester Metropolitan University, Senior Lecturer

Monday 25th January 2021

Cyber criminals publish more than 4,000 stolen Sepa files

The Scottish Environment Protection Agency was hit by a ransomware attack on Christmas Eve 2020. 1.2GB of files were exfiltrated and encrypted. Sepa decided not to pay the ransom offered by the Conti group and the files were subsequently released on the dark web. Some of the data disclosed was already publicly available, but the disclosure also included private contracts, strategy documents, and databases. Sepa's services are continuing to operate and an investigation is ongoing. Read more>

Malware found on laptops handed out to school kids

Malware has been detected on laptops given to school children by the UK government. As part of an ambitious plan to give one million laptops to disadvantaged pupils to aid in remote learning, the government has already given away 800,000 devices. A small number of these have been found to be infected with the Gamarue.I worm, which spies on the victim and sends data to servers in Russia. An IT supplier in the South-East of England is thought to be responsible, but no definitive statement has been made yet. Read more>

Another ransomware now uses DDoS attacks to force victims to pay

Ransomware operators are expanding their methods of extorsion. As well as demanding payment for the encryption keys, some groups have begun launching DDoS attacks on the target as well. An outage of their website would put further pressure on an organisation that would be looking to remove malware and recover from backups. Paying the ransom may seem like the least painful option. When the Maze group combined ransomware with a threat to disclose a copy of the data they had exfiltrated, many other groups copied the approach. It is possible the same may occur with this combined ransomware-DDoS extorsion. Read more>

SonicWall firewall maker hacked using zero-day in its VPN device

The firewall maker SonicWall and issued an announcement of a 0-day vulnerability of two of their VPN devices. Threat actors have been able to leverage the vulnerabilities to gain access to internal systems. Customers have been advised to configure their devices to only allow connections from approved IP addresses. Read more>

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