Greater Manchester | Greater Security | Greater Business

Cyber Foundry

Security News of the Week

by Thomas Martin, Manchester Metropolitan University, Senior Lecturer

Monday 4th January 2021

The Institute for Security and Technology (IST) Launches Multi-Sector Ransomware Task Force (RTF)

A number of high-profile tech companies have joined forces to create the Ransomware Task Force. The non-profit group includes Microsoft, Citrix, and Team Cymru, and will aim to provide recommendations to help reduce the risks posed by ransomware. The task force is part of the Institute for Security and Technology. Read more>

Contact Form 7 5.3.2

A vulnerability has been discovered in a popular WordPress form. Contact Form 7 allows file uploads and has filters to ensure only suitable file types are allowed (e.g. image files). However, including a backslash character can confuse the filter, meaning a file names "xyz.php\t.jpg" would be seen as an image by the filter but interpreted as a valid script once on the server. The plugin has over 5 million active installations, all of which could be vulnerable. WordPress does have an option to enable auto-updates of WordPress and plugins, but as they mention on their site there can be issues with compatibility. Read more>

New SUPERNOVA backdoor found in SolarWinds cyberattack analysis

In a previously reported incident, Orion had discovered they were the victim of a supply-chain attack. An adversary had managed to get a modified version of their SolarWinds code distributed to thousands of their customers (including several US Government agencies). It now appears that SolarWinds has had a second backdoor. The deliberate and carefully executed manner in which the backdoor was deployed indicates the actions of a sophisticated and well-resourced threat actor but is believed to be a separate group from the one responsible for the earlier attack. Read more>

"Is it you in the video?" – don't fall for this Messenger scam

In a new variant of a phishing attack, fraudsters are sending tempting messages via IM. From one compromised account, the fraudster will send to every friend/contact a blank thumbnail with the question "Is it you in the video". Anyone clicking on the thumbnail will be taken to an imitation Facebook homepage that tries to obtain the user's username and password. On providing them, the victim is then passed on to further scam pages, such as VPN and cheap phone offers (with a view to obtaining the victim's credit card details). Users are advised to use 2FA and be vigilant of suspicious messages, even those that appear to come from trusted contacts. Read more>

European Union
European Regional
Development Fund

Manchester Metropolitan University

MANCHESTER 1824
The University of Manchester

University of Salford MANCHESTER

Lancaster University