Greater Manchester | Greater Security | Greater Business

Cyber Foundry

Security News of the Week

by Thomas Martin, Manchester Metropolitan University, Senior Lecturer

Monday 12th October 2020

Microsoft releases tool to update Defender inside Windows install images

Large organisations will often need the ability to deploy hundreds of new systems at a time. Typically, these will take the form of a single image that can be mass deployed. The older the image, the more updates it will need to be able to defend itself, particularly the malware signatures for Microsoft Defender. Microsoft has just released a tool that allows administrators to patch such an image with the most recent Defender package, limiting the window of vulnerability a new system faces when installed. Read more here>

Microsoft Exchange 2010 End of Support and Overall Patching Study

Rapid7 have been scanning the internet to determine how many Microsoft Exchange servers are operating and what their respective patch levels are. They found that approximately 60% of servers are unpatched. This makes the vulnerable to attack, including remote code execution. Many servers have not received patches in years, some not at all. Read more here>

RainbowMix apps generate $150,000 in daily ad fraud profit

Fraudulent advertising earned the creators of the RainbowMix family of apps an estimated $150,000 a day! The apps are mainly low-quality games but included the ability to show ads (even when the app was not active) and appear as other more legitimate apps. In total, they accumulated over 14 million installations. Following the reporting, Google removed the apps from the Play store. Read more here>

TrickBot botnet targeted in takedown operations, little impact seen

TrickBot botnet targeted in takedown operations, little impact seen Several major actors in cybersecurity (including the US DoD, Microsoft, and ESET) have been taking actions to disrupt the TrickBot botnet. Several Command and Control (C2) servers have been taken offline. Some infected machines are receiving updates telling them that the C2 IP address is 127.0.0.1. TrickBot has managed to infect over a million computers, and there is a concern that it may be able to retain some control of the network of devices. Read more here>

Apple T2 security chip fatally flawed

Researchers at ironPeak Consulting have disclosed security flaws with Apple's T2 security chip. The good news is that any attack exploiting this would need physical access, and also that data encrypted in FileVault2 could not immediately be decrypted. The bad news is that any unsigned code could be installed and run with full root privileges (including a keylogger to retrieve any FileVault password). Apple have not commented on the vulnerabilities, but as the problem is in hardware patches are unlikely to be possible. Read more here>

European Union
European Regional
Development Fund

Manchester Metropolitan University

The University of Manchester

University of Salford MANCHESTER

Lancaster University