Greater Manchester | Greater Security | Greater Business

Cyber Foundry

Security News of the Week

by Thomas Martin, Manchester Metropolitan University, Senior Lecturer

Monday 8th February 2021

Free coffee! Belgian researcher hacks prepaid vending machines

A security researcher in Belgium has discovered a way to get free coffee out of Nespresso vending machines. The vending machines use NFC cards to store users' credit and use an obsolete encryption algorithm (Mifare Classic) to protect the balance. As the key size is only 48 bits, it has not been considered sufficiently secure for use for many years. However, the researchers were able to devise an attack that completed in seconds and needed only 8MB of RAM. The researcher responsibly disclosed the vulnerability to Nespresso who have mitigations available for coffee vendors to protect against the attack. Read more>

Over 3 billion emails and passwords hacked in possibly the largest breach ever

A massive collection of over 3 billion emails and passwords were leaked onto a popular hacking form. The leak is a combination of previous leaks from platforms such as Netflix and LinkedIn, rather than the result of a new breach. The scale of the database, and the frequency of password reuse, has resulted in the broad recommendation that everyone update their passwords on all platforms. The generally agreed best practice is to use two-factor authentication where available and a password manager to ensure complex unique passwords can be used for every site. The "have I been pwned" services is considered a trustworthy place to check if one's email address has appeared in any leak. Read more>

Google bans another misbehaving CA from Chrome

Google has decided to remove support for the Spanish Certificate Authority (CA) Camerfirma, effective mid-April. Camerfimra was given six weeks to defend a list of 26 incidents ranging from March 2017 up to January 2021 but failed to satisfy Google's concerns. With between 60%-70% of the browser market, a ban from Google is devastating to any CA, and has led to previous CA's going out of business. There has been no word if other browsers will follow Google's lead, but it is likely. Read more>

With one update, this malicious Android app hijacked millions of devices

A Barcode Scanner app has been discovered to be delivering malicious code to its 10 million Android users. Malicious apps often pose as useful utilities while actually delivering obtrusive ads or spying on the user (typical trojan-type malware). These are often new apps, and short-lived as they eventually get taken down once they draw enough attention from Google. In this case, the app had been behaving well for many years, with lots of positive reviews. However, a malicious update was injected that caused users to complain of unwanted behaviour. The update was signed with the same certificate previously used, making it (at least superficially) indistinguishable from a legitimate update. The app has been taken down from the Google Play store. Read more>

New phishing attack uses Morse code to hide malicious URLs

A targeted phishing attack has been discovered using Morse code. The system (that is over 180 years old) is used to obfuscate URLs of scripts downloaded by malicious attachments. Attackers have many different ways to hide their malicious code, so users have to pay careful attention to URLs, email metadata, and extensions to keep from being infected. Read more>

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