Greater Manchester | Greater Security | Greater Business

Cyber Foundry

Security News of the Week

by Thomas Martin, Manchester Metropolitan University, Senior Lecturer

Monday 28th September 2020

‘Zerologon: instantly become domain admin by subverting Netlogon cryptography (CVE-2020-1472)’

August saw a number of patches released by Microsoft (on Patch Tuesday, 2nd Tuesday of the month), including for their server OSes. Details now coming out about one of the vulnerabilities fixed by the patches, that was rated CVSS 10 (highest possible value). The exploit, “Zerologon”, would allow an attacker to change the Domain Admin password to any desired value, essentially getting full control of the network. Secura initially discovered the issue and admins are encouraged to update as soon as possible. Read here>

‘Privacy-focused search engine DuckDuckGo is growing fast’

The privacy-focused search engine DuckDuckGo is enjoying exponential growth in usage. While they account for only 2% of total searches (compared to Google’s 87%), continued growth could start to put a dent into Google’s monopoly. The rise in popularity is likely due to the frequent news of massive data breaches and growing discomfort with constant digital surveillance by large tech companies. Read here>

‘SMS phishing scam pretends to be Apple “chatbot”’

Despite the growth of popularity of modern messaging apps, SMS is still alive and well. And SMS scams (smishing) still happen. Sophos give a breakdown of a too-good-to-be-true free iPhone 12 offer along with tell-tale signs and precautions to take: Read here>

‘Google App Engine feature abused to create unlimited phishing pages’

The Google App Engine is being misused to facilitate phishing and malware campaigns. The cloud service allows a user to generate any number of subdomains to resolve to the same site. An unintended consequence of this is that attackers can create individual domains sent in links to potential victims. While security systems may flag one, or a small number, of these domains as malicious, there is no limit to the number of alternative domains generated that are seemingly unrelated but resolve to the same malicious site. Read here>

‘Phishing Your Password Manager’

Password managers are a great way to have distinct, strong passwords for many different sites. They use the domain name to determine when they are at the “correct” site, which is usually protects the user from phishing sites. However, when a site uses a Single-Sign On (SSO) system, requests to many different services go to the same domain for login. An attacker can abuse this to phish the password manager for a different set of credentials. Read here>

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