Greater Manchester | Greater Security | Greater Business

Cyber Foundry

Security News of the Week

by Thomas Martin, Manchester Metropolitan University,
Senior Lecturer

Monday 16th November 2020

NAT Slipstreaming

A new type of attack has been announced: NAT Slipstream. Previously, anyone sitting behind a NAT router (which is the vast majority of internet users) enjoys some inherent protection: it is not possible for an attacker to scan/connect to that device. This immediately halts attacks scanning the whole IPv4 address space looking for vulnerable devices. What security researcher Samy Kamkar has discovered is that if a user connects to a compromised website, malicious Javascript can create a new connection back to the user's device, bypassing the NAT firewall. It is possible to disable a feature in the NAT router that is required for the attack to work (ALG – Application Level Gateways) and the major browser vendors are also looking to include methods to block the attack. Read here>

"Instant bank fraud" hoax is back – don't spread fake news!

There are warnings being circulated about the threat of "instant bank fraud". According to these messages, if you so much as click on the link in a received fraud message, you get infected with advanced malware that instantly drains your account. While it is important to be aware of threats and avoid clicking on anything suspicious, this type of attack is almost certainly impossible. The far more likely and common threat is for the link to take you to a phishing page to steal your credentials. Users should have wary of spreading anecdotal stories of threats via messaging/social networks. Read here>

Ticketmaster Hit With £1.25 Million GDPR Fine Over 2018 Data Breach

Ticketmaster have been hit with a hefty £1.25 million fee by the UK's ICO (Information Commissioner's Office). Back in 2018, the third-party chatbot used on their site was compromised to allow an attacker to extract financial details. 60,000 cards were subjected to fraud, and 6,000 more were replaced after suspected fraud. Ticketmaster waited nine weeks after being informed of the possible fraud before they started monitoring their network traffic. Read here>

DNS cache poisoning attacks return due to Linux weakness

A new DNS cache poisoning attack has been discovered on Linux servers. DNS cache poisoning was first discovered in 2008 and was widely considered resolved. A successful attack can cause incorrect mappings of domain name to IP addresses to be saved in a name server, with the potential of causing phishing or spoofing attacks on a large number of victims. This particular attack takes advantage of a side channel to learn the source port that the server is using. Patches and countermeasures are under development. Unfortunately, it has been discovered that Windows and MacOS are also vulnerable to this flaw. Read here>

European Union
European Regional
Development Fund

Manchester
Metropolitan
University

MANCHESTER
1824
The University of Manchester

University of
Salford
MANCHESTER

Lancaster
University