Greater Manchester | Greater Security | Greater Business

Cyber Foundry

Security News of the Week

by Thomas Martin, Manchester Metropolitan University, Senior Lecturer

Monday 28th June 2021

Microsoft admits to signing rootkit malware in supply-chain fiasco

Microsoft have inadvertently allowed rootkit malware to propagate. All kernel drivers in Windows require a signature from Microsoft, who test all submitted code before certifying. However, a security researcher at G Data noticed a valid driver (called "Netfilter") exhibiting unusual behaviour (communicating with China-based Command and Control IP addresses). Further investigation revealed more suspicious behaviour without any clear legitimate functionality. Microsoft admitted to signing the malicious driver. They have suspended the relevant account and are reviewing related submissions for similar signs of malware. Read more>

Microsoft's Halo dev site breached using dependency hijacking

A security researcher managed to successfully gain access to Microsoft's game studio network using a dependency confusion attack. Developers will often make use of libraries of packages when creating software (npm for JavaScript, PyPI for Python, etc.) which can be public or private. However, if the name of an intended private package matches the same name on a public package, then it is possible the public package will be loaded and run instead. In this case, the researcher found a reference to a package name that did not appear to match any existing public package, created his own, and it was later deployed from inside the Microsoft network.
Read more>

WD My Book NAS devices are being remotely wiped clean worldwide

The Western Digital My Book Live NAS is a standalone device intended to provide a reliable backup for important data. However, users have been discovering their devices suddenly empty and inaccessible. It was discovered that affected devices had been issued a factory reset command. Some users were able to use file recovery software to recover some files (a factory reset does not actually overwrite the data, just marks it as available), but such steps are elaborate and not guaranteed. It is believed that the devices were directly accessible over the internet (either using a static IP address or port forwarding in a NAT network) which allowed an attacker to exploit a remote code execution vulnerability. Since the My Book devices provide their features through a cloud service, such direct connection is not actually necessary. Read more>

Dell SupportAssist contained RCE flaw allowing miscreants to remotely reflash your BIOS with code of their creation

Security firm Eclypsium have discovered a chain of vulnerabilities with Dell's SupportAssist which could allow an attacker to remotely reflash a tampered BIOS. As the BIOS operates below the operating system, it has the capability to undermine any of its operations. The initial issue with the SupportAssist tool is that it did not properly validate the TLS certificate as coming from the downloads.dell.com domain (it accepts any domain so long as it has a valid certificate). While the level of access the attack grants is concerning, the complexity of the attack is likely enough to put off all but the most determined adversaries. A patch is available for SecureAssist which will mitigate the issue, as will remove of the tool. Read more>

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