FUJITSU

Monthly Cyber Threat Intelligence Bulletin

A group claiming to be part of the international hacking network, Anonymous, has reportedly managed to take control of Victoria's Human Rights Commission website and used the page to post a nonsensical message about its social network, AnonPlus. The message stated that the group is "non-criminal" but questions are still being asked as to why the commission's website was targeted.
http://www.scmp.com/news/asia/australasia/article/2058897/anonymous-hackers-hijack-australian-states-human-rights

A software engineer reported on christmas day that his smart TV from LG had been infected with ransomware, and was demanding $500 to unlock the device. IoT ransomware will occur more in the future with household items being targeted including the likes of fridges, TVs etc.
http://securityaffairs.co/wordpress/54991/malware/lg-smart-tv-ransomware.html

This week Google Brazil seem to have been DNS hijacked, and defaced by the lone hacker going by the name of "Kuroi'SH." Google Brazil immediately tried to restore the hacked website but seemed unable to gain control as the domain, Google.com.br is still unavailable to visitors. According to reports in Brazil media, the Google Brazil users were getting the defaced message from Kuroi'SH for a whole 30 minutes before Google took the website offline.
http://www.techworm.net/2017/01/google-brazil-hacked.html

This week GCHQ have gone on a hiring spree in which they have spent £422,073. The recruitment drive comes after senior Conservative MP Andrew Tyrie, who chairs the Treasury Select Committee, called on the head of the NCSC to make cyber defence of financial services industry a top priority. The National Cyber Security Centre (NCSC) is looking to recruit desk officers, team leaders, a deputy team head and strategy and impact lead. http://www.ibtimes.co.uk/gchq-unit-422000-hiring-spree-defend-uk-economy-cyberattacks-1599647

Many companies have figured out that they can avoid paying these ransoms by wiping a system clean, restoring it with backup drives, and going about business without being held hostage. But as a result of increased ransom-avoidance, cybercriminals have created an even more insidious threat. Imagine malware that combines ransomware with a personal data leak: this is what the latest threat, doxware, looks like. http://www.darkreading.com/attacks-breaches/ransomware-has-evolved-and-its-name-is-doxware/a/d-id/1327767

It has been discovered this week that the inflight entertainment system from Panasonic contains a large amount of vulnerabilities that would allow an attacker to control what passengers see and hear on their in-flight display. This inflight entertainment system is used by large airlines including the likes of United Airlines, American Airlines, Virgin Atlantic, and Air France. This has hit the top target list as many media and security researchers are also discussing the likelihood of exploiting these vulnerabilities and then moving laterally into other systems in-flight. http://www.darkreading.com/vulnerabilities---threats/panasonic-inflight-entertainment-system-vulnerable-to-attack/d/d-id/1327768?_mc=RSS_DR_EDT