April 2019

HACK LIFE

Risk Factory's Monthly Information Security Awareness Bulletin

STORY OF THE MONTH: YET ANOTHER PRIVACY 'CLUSTERZUCK'

Each month, when the time for creating the monthly newsletter comes round, we consider all of the previous months stories and try to find one that will resonate and be of interest to as wide a group as possible. So while, the thought of pace makers being hacked will be literally of critical importance to some, it's not going to pique the interest of the broader cross-section of readers. But listen, we really don't want every other headline to have Facebook in the title but they make it so easy! So here we are, yet again – this time they've been storing our passwords in plain text format and they've been doing it in the 100's of millions. Not only is this an obvious vulnerability to an external attack, it means that user passwords are at the mercy of Facebook employees who had internal access to the data. In this case, around 20,000 of them. How confident are you that not one of those 20,000 wouldn't be susceptible to a bit of dark-web password trading? It's been going on since at least 2012 as well. Oh yeah, it's not just Facebook but their 'lite' version as well and Instagram. Their advice? Change your FB & Instagram passwords. Our advice? Don't go on Facebook ever, but if you must, change not only FB passwords but also any other account which used the same passwords. By the way, please use different passwords for every single account. Ask us if you need more advice.

DID YOU KNOW?

Monday 25th March heralded not only Apple's latest fanfare of goodies to get all their fans to dig even deeper into their pockets but also the arrival of iOS 12.2 with over 50 patches to fix flaws, some of them pretty hefty security related ones, one of them being a malicious application that allows microphone access unbeknown to the device owner.

RESOURCE OF THE MONTH

Do you own an ASUS machine? If so, you need to know that over 1 million ASUS computers were infected with malware via an official ASUS live automatic software update between June and November of last year. ASUS was notified of this at the end of January this year according the folks at Kaspersky Labs , who first identified the hack in the wild. They have also created a tool which you can download that'll identify if your machine has been targeted. You'll find it in the link above.

MONTHLY QUIZ

What James 'Bondish' type tech is able to detect radioactivity? Clue: It's not Geiger Counters! Email us your answer and our winner will be chosen randomly from correct answers and will win a HACK LIFE t-shirt! ***info@eriskology.com***