May 2019

HACK LIFE

Risk Factory's Monthly Information Security Awareness Bulletin

STORY OF THE MONTH: O365 PHISHING ATTACKS: CRITICAL INFO

Sometime earlier this year, we had a call from a client wanting to refer one of their clients to us. The client had suffered what some call CEO Fraud or Spear Phishing and some refer to as Whaling. Regardless of how you label such an attack, the modas operandi is always roughly the same: Someone in accounts gets an email purporting to be from a senior executive, requesting an urgent payment is made to a 3rd party supplier. We've since had a worrying number of these coming through, initially we thought it was a vulnerability being exploited in O365 (which would have had huge connotations), then we thought it was just a case of senior executives being free and easy with their credentials but recently it has transpired that hackers are getting previously compromised credentials from the dark web and using those passwords to take over O365 accounts of the execs. The reason they have been so successful is simple – these execs used the same password across multiple accounts – the attackers were able to count on the fact that a significant percentage of their potential victims would use the same password on for their O365 account as they did for the compromised one. Often the attackers would monitor these email accounts, unnoticed, for months – gathering intel to make the attack all the more convincing and devasting. Simple advice to stop this happening? Always use a unique password for every account.

DID YOU KNOW?

If your business requires that you change your passwords regularly you could be playing into the hands of attackers? When asked to change their password, hard pressed users will often just add a single character – usually a number that changes incrementally with each change, so for example Ecl1p$E will become Ecl1p$E1, Ecl1p$E2 and so on. This is a bad thing. Not only is it a rubbish password to begin with, but hacking software can easily be configured to add the extra number as part of its brute force cracking methodology.

RESOURCE OF THE MONTH

Google Chrome now has an extension you can add called 'Password Checkup' Whenever you sign in to an account with a password and username it will tell you if those credentials are no longer safe due to a known breach!

MONTHLY QUIZ

Which Government department, much lamented by George Harrison has fallen foul of the GDPR? 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***