Efficacious Tactics, Mechanics and Heuristics for Progressive Social Engineering

Ujas Dhami[1]

[1]Department of Computer Engineering, Silver Oak University

June 21, 2021

Abstract

With increasing digitalization and company infrastructure over the years, the attack vectors in computer security have been enormously metastasizing. In scope, several breaches and intrusions have been dominantly carried out by one common tactic, Social Engineering. The domain has gained momentum over the years in successful compromisation of assets. Metrically, Social Engineering proportionately, has been considered one of the most dangerous weapons of any threat actor and consecutively, one of the most dangerous threats to any company's human resources. As per Cobalt's Cybersecurity Statistics of 2021, 61% of organizations globally, have faced breaches carried out by Social Engineering attacks. Moreover, proofproint 2021 State of the Phish Report recognizes Social Engineering attacks as emerging attacks with devastating potential. These type of attacks are often undervalued by employees and the IT staff for majority of the companies. This paper will brief about the new tactics I used, as a threat actor, endeavouring to make the most out of a persuasive conversation, involving (i) physical hooking, (ii) telephonic attacks, and (iii) neuro-anatomical deductions briefing how the existing Social Engineering attacks can emulate the neurochemical processes inside the brain.

Hosted file

Efficacious Tactics, Mechanics and Heuristics of Progressive Social Engineering.pdf available at https://authorea.com/users/420739/articles/527006-efficacious-tactics-mechanics-and-heuristics-for-progressive-social-engineering

1