Social engineering, drive by download attack

7 Elements was engaged to deliver a multiple scenario social engineering engagement. The primary objective was to entice different parts of the business to click on a link (under 7 Elements' control) in order to assess the exposure to so-called "drive-by downloads" and other client-side attacks.

7 Elements utilised a number of different Open Source Intelligence (OSINT) gathering techniques, including search engine and social network analysis, to map out an organisation chart of our target. The information gathered through social network mapping transpired to be 95% accurate - a demonstration of the power of this type of information gathering. Using this organisation chart we were able to identify targets in different departments and develop different attacks in order to achieve our objective.

Our most successful attacks involved impersonating a local university student performing research in order to gain trust and build credibility, resulting in the successful completion of our questionnaire by numerous employees. The questions related to internal security controls as well as establishing the ability to conduct browser based exploitation. We also had great success through the use of social media in order to engage with employees of the company and establish rapport and trust.

We conducted five different scenarios and in four out of the five we achieved our objective. In total, approximately 30% of all links sent were clicked on by their target. Our client has since worked with us to improve the security awareness training it provides to all staff and has incorporated examples and output from our assessment into this education programme.