Joshua Farias

Professor Ramella

SEC 431

5th December 2023

Social Engineering

Social engineering is a method of manipulation employed by threat actors to deceive and exploit individuals, targeting human psychology rather than technology itself. Threat actors often use open-source intelligence (OSINT) to gather information about their potential victims. What threat actors learn through OSINT is then used to design their social engineering attack to suit the interests of a particular individual or corporation. A threat actor will often exploit their targets by appealing to their emotions (trust, fear, curiosity, and greed) with the hopes of making the person act impulsively without investigating further.

For instance, a threat actor could leverage OSINT and discover that an individual is into trading cryptocurrencies and that they use the Blockchain exchange. A threat actor could unearth this by analyzing their posts on a social media platform that also contains their email address. Recent posts suggest that the individual expressed concerns over security breaches on a different cryptocurrency exchange. A threat actor could use this information they gathered from the individual to send them a phishing email prompting them to change their password for Blockchain due to an “attempted security breach” preying upon the security concerns they expressed on their social media page.

The Social Engineering Toolkit would be used to copy the HTML and CSS from the login page from Blockchain, host it on a command-and-control server and have it responded back to the threat actor with the credentials once the user entered them on the fake site. This exploit is a combination of both technology and non-technology tactics as the threat actor creates a fake website and sends out a legitimate looking email while also trying to manipulate the target's actions based on what they gathered from open-source intelligence. Threat actors may also try to incorporate additional layers of deception such as spoofed email addresses, security certificates to try and make the email and website come across as legitimate.

With regards to countermeasures that can be employed to mitigate risks associated with social engineering attacks, multi-factor authentication is crucial in providing another layer of safety. For instance, if the user from the example provided earlier had MFA enabled on their Blockchain account even though the attacker obtained the password, they would not be able to access the account without the additional authentication to do so. With phishing attacks, many anti-viruses, email filters and firewalls rely on blocklists of known command and control sites making zero-day threats difficult for security software to detect as malicious and block even with more advanced security apparatuses such as IDPS systems. Implementing strict access controls and following the principle of least privilege is essential for mitigating the damage that can be done by a social engineering attack. While technology plays an essential role in facilitating and defending against social engineering attacks, the human element remains the most critical factor which is why end-user education in identifying social engineering attacks is essential in reducing vulnerabilities.