The Art of Hacking Humans: Intro to Social Engineering

Baiting

Baiting uses a form of enticement to lure unsuspecting victims into installing malware on their endpoint and/or network. An example is clickbait that is common on video sites like Youtube where a video has a thumbnail that elicits the curiosity of individuals leading them to view the video, only to discover that the thumbnail has little or no correlation to the video. Such techniques are used on Youtube and the likes to bring traffic the video uploader whether for the number of views or to viewers to see the video which could be an advert or promotion or something like that or just a prank. However, the baiting can have more sinister applications like malware infections as stated.

Baiting can come in the form of messages (whether email, social media or SMS), flashing banners, pop-up messages, or carefully placed or labeled storage media. Baiting by way of messages normally comes with an enticing link or attachment which contains malware that can infect victims compromising the victims' systems and probably organization/network or links could be used to direct victims to a fraudulent site (this means phishing messages are a form of baiting, as they use enticement in the form of links and attachments. Some websites or apps may have flashing banners or pop-up messages that attract victims' attention and curiosity, like job opportunities, a way to make quick money, pornography, malware detection and so on, which when clicked lead to compromise of endpoints and networks. The way of baiting by way of storage media usually involves the malicious attacker placing storage media like flash drives, optical disks, memory cards and so on in strategic places that could be easily noticed by an organizations employees; the bait might be labeled with enticing labels like senior management payrolls or bonuses, promotion lists, systems update, anti-virus, even pornography to get the employees to try viewing what is on these media on their endpoints, resulting in malware infection of systems and the network.

Panda Security (2012) detected a Facebook worm that was spread by way of bait claiming to be a leaked video of a celebrity couple's home. When victims clicked the video, instead of playing it leads them to a fraudulent Facebook page asking them to install a plug-in that would enable them view the video which would get the victims infected and the bait is shared with all the victim's contacts (Panda Security, 2012). Another example was a Facebook clickbait worm described by Souza (2015) which came in the form of an article as bait. When the article is clicked a pop-up message comes asking to like the article's Facebook page with an "X" button on the top right corner supposedly signifying a cancel button, liking would initiate malware infection same as canceling; that is to say anything clicked on the pop-up is a bait leading to infection. Similarly, this malware also shares the bait to all the victim's Facebook friends.

Figure 3: Sample baiting email

Baiting primarily takes advantage of human curiosity. It also takes advantage of human weaknesses like desire, lust, greed and desperation. Bait like those claiming to lead to relationships like dating sites and pornography take advantage of desire and lust; get rich quick bait takes advantage of greed; while those offering job opportunities could take advantage of desperation and helplessness. Low self-esteem may also be manipulated with quick weight loss or beauty enhancement bait.

Baiting attacks can best be avoided by awareness. Other factors that can help protect against falling victim of baiting include self-control, patience, and improved self-esteem.

References:

Panda Security (2012) *Katy Perry and Russel Brand Used as Bait to Spread New Facebook Worm, According to Panda Labs* [Online]. Available from: https://www.pandasecurity.com/mediacenter/press-releases/katy-perry-and-russell-brand-used-as-bait-to-spread-new-facebook-worm-according-to-pandalabs/ (Accessed: 2 November, 2017).

Souza, F (2015) *Analyzing a Facebook Clickbait Worm* [Online]. Available from: https://blog.sucuri.net/2015/06/analyzing-a-facebook-clickbait-worm.html (Accessed: 2 November. 2017)