The Art of Hacking Humans: Intro to Social Engineering

Chain Messages

We had seen earlier that chain letters of old had evolved into modern day chain messages using communication media like email, social media and SMS to proliferate by malicious attackers to achieve their malicious goals. Chain messages are messages sent using various communication media which lead victims to spread the message to others leading to an exponential increase in the spread of such messages. Sometimes these messages keep circulating for many years. Malicious individuals use chain messages to achieve varying goals: a chain message can be used to spread malware or compromise victims using phishing techniques; mislead victims into damaging their systems; spread things like malice, mistrust, fear, confusion or stir public opinion; get email addresses to use for further attacks and so on. Chain messages are usually based on some kind of sentiment, belief, superstition or just fun. They tend to end with an encouragement to forward to other people (some even request copying the sender when forwarding), or come in a format that the victim cannot help but forward to other, who would similarly do the same.

Some chain messages that have been circulating, usually through email and other text-based messing media, include phishing links or attachments. The messages are usually for something like viru interest. Recipients might immediately forward such messages to people they feel may find it beneficial even without clicking the links or attachments themselves, but those whom might be in need of what is sent would probably do so and send to more friends and relatives. The links/attachments may result in actual phony pages or documents which would be laced with malware. Virus hoaxes like the jdbgmgr.exe email hoax can ask victims to delete certain systems files by informing them that the file is a virus and they would probably be infected because they are in the sender's mail list describing how to access the file (Christensen, 2017), the file is an actual Windows file and not a virus, so when victims see it, they are automatically convinced they are infected and delete the file. The jdbgmgr.exe was generally harmless, but a malicious attacker can send such a message referring to a crucial security file as a virus, which when deleted makes the victims susceptible to malware infections or provide the attacker easy access to their systems. Such a message is very likely to spread even if there are not instructions to forward to all your contacts, as the initial message informs the victims that they are receiving such because they are part of the sender's mail list, hence they also automatically would forward the message to those on their mail lists as well.

Chain messages could come in the form of a message telling you to forward to others in order to get some good luck or avoid bad luck; could be a joke, health tip, religious advice asking that you should spread to others; if the messages contain links or attachments, there is a possibility of them containing malware for phishing. Some of the messages may end with "forward to other including the person who sent to you", these could be so that they malicious attacker can harvest email addresses as some may even instruct use the reply all option and copy more recipients. The attacker can use this to gain knowledge of who and who are connected and can use that to initiate attacks targeting victims that are within a particular circle of friends. There have been messages claiming to be from Yahoo or similar platforms claiming that your account will be canceled if you don't forward the message informing you to a large number of recipients, eliciting you to use reply all and copy more people, giving the attacker a good database of you and your contacts.

There are chain messages that are initiated to spread some form of propaganda in the grapevine. These types don't target systems, but people. They can be used to influence public opinion, or set people against one another, could lead to civil unrest and things like that. A nation state can use this kind of chain message to direct what happens in another nation state in a certain way, like swings elections in a certain direction, spread mutual distrust setting certain demographics against others, such that things move how this manipulating nation state wants in line with their own interest.

Some weaknesses chain messages take advantage of include lack of awareness, ignorance, willingness to help, sentiments, beliefs and zealousness. The victims will likely circulate chain messages out of lack of awareness and ignorance of what the messages contain and the phenomenon of chain messages as a whole. The victims are usually zealously trying to help out their friend and acquaintances when the forward them out of concern for the recipients. Sentiments in the messages and the belief they appear to promote also ginger victims to spread the messages the more.

Awareness is the best medicine against chain messages. There is a need to think twice before forwarding messages to others and be sure of what the message contains, especially when the message asks you to forward to others, and even more so when asked to copy the sender or use "Reply All" button. You should also bear in mind that organizations like Yahoo are not going to ask you to forward messages to all your contacts or as many people as possible in order to avoid your account being blocked or cancelled.

References:

Christensen, B.M. (2017) *Teddy Bear Virus Hoax - jdbgmgr.exe* [Online]. Available from: http://www.hoax-slayer.net/teddy-bear-virus-hoax-jdbgmgr-exe/ (Accessed: 3 November, 2017).