Dan Wnuk
DSS
2/8/2012

Article Summary 4: Detecting Targeted Malicious Email Using Persistent Threat and Recipient Oriented Features

My final article to summarize comes from the IEEE Security and Privacy Journal, and was written by Rohan M. Amim, Julie J.C.H. Ryan and J. Rene van Dorp. The article starts out by showing the different between malicious email and spam - that is, spam is sent to millions of users and the general method of identifying spam is by using probabilities to decide if an email being received is spam. With targeted email, the emails are only sent to one or a handful of people and so the same techniques do not apply. The purpose of targeted malicious email is to gain access to sensitive data. This can be done by using malicious attachments or giving links to the user that are also malicious, tailoring these links and attachments to that specific user to increase the odds of them opening them. The journal collected a lot of email data and began to analyze the data for certain metrics. First, it measured the amount of emails that received targeted malicious email. The vast majority of accounts analyzed did not have any. From this data, they performed google searches to see which emails are listed on Google, and determined that the ones that are listed on Google were the ones that ended up being targeted. Another trend that they tried to analyze was the position of the people being targeted. They found that the higher level positions were not at the top of the list of people being targeted, but a position in which 44 people had at the company was the third top of their list. This shows that emails aren't even often designed to be sent to the top tier person - possibly assuming someone who didn't have as much responsibility was less intelligent and therefore more likely to fall for whatever tricks they were trying to use.

The next part of the paper goes into ways of detecting the threats. Locale settings can often be seen from where the attacker is sending out the emails, which can help identify potential threats. Additionally, if a person uses a tool to mass send out these types of emails,

the tool can leave a fingerprint in the email itself as well. This would mean that the ability to figure out the fingerprint means the entire tool can be blacklisted. These types of identifications fall under the category of “persistent threat” - that is, clues from the technology can identify it as a threat. The other category is called recipient oriented, which basically means that the email is targeted to a person because their email is more visible due to being a PR person for the company, or being in a high position would mean they have access to more sensitive data. There are a lot of potential clues for detecting targeted malicious email, but as of yet there is no good product that can accurately identify it with any sort of success, likely due to the complexity of analyzing these types of indicators programmatically instead of manually.

Overall, this article taught me a lot about ways of classifying threatening emails. Currently there are no good products that can accurately identify targeted malicious emails (versus spam emails), so it might be a good industry to start up in in the hopes of starting a big company. This could provide focus to my development. Extracting this out to general principles, it shows that there are often algorithms that can be applied in a lot of situations, especially in terms of data mining to predict future data, such as in this industry. Also, being more aware of the possible indicators for receiving these types of messages will make it easier to avoid them. The article was a good read and is something I am genuinely interested in.