# Identify the risk strategies that the actors can adopt to tackle the problem

In this section the risk strategies of the actors described in the previous section will be discussed. These actors are the botnet masters, the consumers, businesses, money mules and the malware programmers. The sociotechnical nature of the system ensures that these actors have different and even conflicting strategies. These conflicting strategies will be pointed out and the change of these strategies throughout will be given.

The botnet masters control the botnet via C&C. It is the only way for them to communicate with the bots. It is essential that the C&C is protected because without it the botnet masters can’t reach their network and thus make money. To reduce the risk the botnet master should use a way to communicate to the bots via the C&C that anti-virus/malware software will not detect. One popular C&C communications technique is to use publicly available DNS servers rather than the systems inside a private network. Advanced-persistent-threat actors try to use public DNS services to avoid logging within the private network and risk detection. (James Ringold, 2014) The goal to protect the C&C servers is the direct opposite of what the problem owners, mentioned in the previous section have namely, to disrupt the C&C. The consumers and business also have conflicting strategies because they are the ones targeted.

Strategies used by consumers are listed in the category risk mitigation and risk transfer. The consumers can mitigate the risk by installing firewalls, make back-ups and don’t open untrustworthy emails. Consumers can also transfer the risk toward the ISP. In this case a contractual agreement of financial compensation with the ISP is formed.

Businesses are targeted a lot by SPAM, The annual cost due to loss in productivity through spam is estimated to be around $20 billion. This is because a percentage of an employee’s time is spent browsing and deleting individual spam messages during a given day at work. (Malik A. Feroze, 2015) Businesses have a lot of the same risk strategies as the consumers but cannot accept certain risks for legal reasons. To make sure privacy data of costumers and other sensitive data is not leaked, employees should be trained in recognising SPAM. A proactive strategy, such as staff training and adoption of innovative strategies in a timely fashion, can yield significant benefits at reasonable costs. (Brent Rowe, 2006)

Money mules make the withdrawals from the bank accounts the money generated by the botnet are transferred to. The names of the botnet masters or the money mules are not registered to these bank accounts which leave them anonymous. The withdrawals are physically done at ATMs which make them irrelevant for cyber security risks strategies.

Malware programmers are the coders that create the C&C’s and write the code that infects the machines. Malware use various techniques to camouflage them to not be easily visible and make their lifetime as longer as possible. Although, camouflage approaches cannot fully stop the analysing and fighting against the malware, but it make the process of analysing and detection prolonged, so the malware can get more time to widely spread. (Babak Bashari Rad, 2012) To reduce the risk to get their malware detected the programmers need to keep investing in new techniques to camouflage the malware.

The actors described above have clear opposite interest concerning SPAM. On the one hand there are the criminals and on the other hand there are the actors targeted by the criminals. The constant change in threats and vulnerabilities ensures that all actors have to change their risk security strategies throughout time.

Bibliography

Feroze, M. A., Baig, Z. A., & Johnstone, M. N. (2015). A Two-Tiered User Feedback-based Approach for Spam Detection. *ICSNC 2015*, 22.

Rad, B. B., Masrom, M., & Ibrahim, S. (2012). Camouflage in malware: from encryption to metamorphism. *International Journal of Computer Science and Network Security*, *12*(8), 74-83.

Ringold, A. R. (2014, June). *Command-and-control servers: The puppet masters that govern malware*. Opgehaald van Techtarget.com: http://searchsecurity.techtarget.com/feature/Command-and-control-servers-The-puppet-masters-that-govern-malware

Rowe, B. R., & Gallaher, M. P. (2006, March). Private sector cyber security investment strategies: An empirical analysis. In *The fifth workshop on the economics of information security (WEIS06)*.