Multi-Covert Channel Exfiltration Techniques

Mahdi Akil
Department of Computer Science
Karlstad University
Karlstad, Sweden
mahdi.akil@kau.se

Luigi V. Mancini
Dipartimento di Informatica
Universita di Roma Sapienza
Rome, Italy
mancini@di.uniroma1.it

Daniele Venturi
Dipartimento di Informatica
Universita di Roma Sapienza
Rome, Italy
venturi@di.uniroma1.it

Abstract

Frequently, it is believed that the adoption of encryption is adequate to ensure the safety of the message. However, encryption only restricts unapproved individuals from decoding the message. Whereas in many circumstances, the mere presence of communication or variations in communication patterns, such as an increase in message rate, is sufficient to raise doubt and initiate alerts. One of the best ways to bypass that is by using covert channels. In this paper, we create innovative protocols that use multiple covert channels working in parallel to exfiltrate data from a remote-controlled machine to our server. The provided protocols guarantee the completeness and unforgeability of the exfiltrated data. We analyze the difference in performance between the created protocols and provide mathematical equations to evaluate them.