0.1 INTRODUCTION

Data exfiltration, data extrusion or data exportationis the unauthorized, illegal and unapproved removal of data from a computer or a network. We have two types of data exfiltration, it could be manual where the attacker has physical access to the computer or it could be automated by a malicious program running over the network. As it requires the transfer of data inside and outside a company's network, it frequently mimics typical network traffic, allowing valuable data loss events to go unnoticed until data exfiltration has already been completed. And when your company's most precious information is in the hands of hackers, the damage is limitless.

There are more data exfiltration ways than there are roads to Rome. but still, the most sufficient way to exfiltrate data is by using covert channels.

Lampson first described covert channels [**?**] as "Channels not intended for information transfer at all". Since then the definition of covert channels has been developing. In 1993 Virgil Gligor defined them [**?**] as "A communication channel that allows a process to transfer information in a manner that violates the systems security policy". While the most recent definition was given in 2010 by Eric Couture [**?**], he described a covert channel as "A mechanism for sending information without the knowledge of the network administrator or other users". To sum all this up we can describe covert channels as "A Communication technique that is used to transfer information in a secretive and unauthorized manner. Hence, it's simply an extra way for information to leave a network".

Data Exfiltration using a covert channel can be expressed as a bag with a secret section that a spy is using to slip a weapon past security guards into or out of a guarded building. An attacker can use covert channels to transmit sensitive documents unobserved. In our case, rather than bypassing security guards we need to bypass network security standards to implement a covert channel. And just as a spy can use that same secret section to sneak a weapon from security guards when entering a guarded building, an attacker can use a covert channel to conceal a cyber weapon. For example, download a malware from an external server into the victim machine within an organization's private network.