**White-List DataSet : POC**

A *whitelist* (or white list) is a list or register of entities that, for one reason or another, are being provided a particular privilege, service, mobility, access or recognition. As a verb, to whitelist can mean to authorize access or grant membership. Conversely, a blacklist is a list or compilation that identifies entities that are denied, unrecognized, or ostracized.

If we were to create a Dataset around this POC, we’d start with creating a list of commonly used and “accept” programs (I.E. Evernote,dropbox,teamviewer,etc…)

Next, we’d create a list of IPs or/and, SSL fingerprints/certificates, and common net speeds associated with these external connections.

The value of this Dataset would be to offset the false positives typically experience when utilizing BlackList Data. In the case of IPS, a false positive can be detrimental to the availability of some resource at that specific point in time.

The “NetSpeed” can be done in several different ways. We can attach a “risk\_level” that quantifies normal usage between the whitelist service and external IP. When there is an outlier in net speed/usage on that whitelisted IP, an alert can be generated to bring the user’s attention with the irregular usage/interaction with said IP. One of the values of this particular “header”, used to combat APT/Malware utilizing overt channels for data exfiltration.

An *overt channel* is the normal and legitimate way that programs communicate within a computer system or network. A *covert channel* uses programs or communications paths in ways that were not intended.

Trojans can use covert channels to communicate. Some client Trojans use covert channels to send instructions to the server component on the compromised system. This sometimes makes Trojan communication difficult to decipher and understand. An unsuspecting intrusion detection system (IDS) sniffing the transmission between the Trojan client and server would not flag it as anything unusual. By using the covert channel, the Trojan can communicate or "phone home" undetected, and the hacker can send commands to the client component undetected.