Early Prediction of Network Protocols in the Forensic Analysis of DNS Tunneled Traffic

Irvin Homem*, Panagiotis Papapetrou, Spyridon Dosis, Stylianos Gisdakis
{irvin, panagiotis} @dsv.su.se; {dossis, gisdakis} @kth.se

In recent years there has been an increase in the use of DNS tunneling techniques for perpetrating malicious activity such as data exfiltration and malware communication. Network security mechanisms struggle to detect such activity. Network forensic analysis has been a source of respite, however it is slow and effort intensive. Furthermore, Network Forensics Analysis Tools (NFATs) struggle to deal with undocumented or new network tunneling techniques. In this study we present a method to aid forensic analysis through automating the inference of protocols tunneled within DNS tunneling techniques. We analyze the internal packet structure of DNS tunneling techniques and characterize the information entropy of different network protocols as well as their DNS tunneled equivalents. From this we present our protocol prediction method that uses statistical pattern matching techniques on information entropy distributions. Finally we analyze the performance of our classifier and show that it has a prediction accuracy of 75%. Our method also preserves privacy to some extent as does not parse the actual tunneled content, rather it only calculates the information entropy.