

A Survey of Domain Name System Tunneling Attacks: Detection and Prevention

Authors : Lawrence Williams

Abstract : As the mechanism which converts domains to internet protocol (IP) addresses, Domain Name System (DNS) is an essential part of internet usage. It was not designed securely and can be subject to attacks. DNS attacks have become more frequent and sophisticated and the need for detecting and preventing them becomes more important for the modern network. DNS tunnelling attacks are one type of attack that are primarily used for distributed denial-of-service (DDoS) attacks and data exfiltration. Discussion of different techniques to detect and prevent DNS tunneling attacks is done. The methods, models, experiments, and data for each technique are discussed. A proposal about feasibility is made. Future research on these topics is proposed.

Keywords : DNS, tunneling, exfiltration, botnet

Conference Title : ICCSCIT 2023 : International Conference on Computer Science, Cybersecurity and Information Technology

Conference Location : New York, United States

Conference Dates : January 30-31, 2023