DNS AS C2

The attackers use DNS as a C2 channel.

DETECTION

Network Threat Hunting - Zeek/RITA Analysis
Firewall Log Review

TOOLS

dnscat2

https://www.blackhillsinfosec.com/bypassing-cylance-part-2-using-dnscat2

Backdoors & Breaches

C2 and EXFIL