Domain Fronting as C2

The attackers use Domain Fronting to bounce their traffic off of legitimate systems.

DETECTION

Network Threat Hunting - Zeek/RITA Analysis
Firewall Log Review

TOOLS

Cobalt Strike

COBALT STRIKE
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS

https://www.cobaltstrike.com

https://www.blackhillsinfosec.com/bypass-web-proxy-filtering

Backdoors™ & Breaches

C2 and EXFIL

Created by: **BLACK HILLS** | Information Security