Traffic Signaling

The attackers use specific fields in TCP/IP packets to activate their backdoor.

DETECTION

Endpoint Security Protection Analysis
Endpoint Analysis
Network Threat Hunting - Zeek/RITA Analysis

TOOLS

Winnti
Umbreon

https://attack.mitre.org/techniques/T1205

EXPV1_0421

Backdoors™ & Breaches

C2 and EXFIL

Created by: BLACK HILLS | Information Security