HTTP as Exfil

The attackers use HTTP as an exfil method. This is usually used in conjunction with some type of stego. For example, VSAgent uses base64 encoded __VIEWSTATE as an exfil field.

DETECTION

Network Threat Hunting - Zeek/RITA Analysis
Firewall Log Review

TOOLS

Metasploit Reverse HTTP Payloads
C2 Matrix

https://www.thec2matrix.com/

CDV2_0421

Backdoors™ & Breaches

C2 and EXFIL

Created by: BLACK HILLS | Information Security