HTTPS as Exfil

This is pretty basic: the attackers use HTTPS. Lots and lots of malware uses this. For example, Meterpreter has used this technique for a long time. It can be used in conjunction with other stego techniques.

DETECTION

Network Threat Hunting - Zeek/RITA Analysis
Firewall Log Review

TOOLS

Metasploit Reverse HTTPS Payloads
SILENTTRINTY

HeTvTiPlS

https://www.metasploit.com

https://attack.mitre.org/techniques/T1573/

https://github.com/byt3bl33d3r/SILENTTRINITY

Backdoors™ & Breaches

C2 and EXFIL

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