Network Indicators of C2/Data Exfil Cheat Sheet

- Spring 2014 Edition -

Network/Generic

FirewallでDenyされる通信が多い
通信先IPアドレスの所在がレアな国（中国、ロシア、エストニアなど）
非標準ポートでの通信（TCP80番以外のHTTPなど）
標準ポートを使った未知プロトコル（TCP80番でHTTP以外など）
通信間隔が一定である通信先IPアドレス/FQDN
外部への転送バイト量が多い
業務時間外の通信

HTTP/HTTPS

プロキシ認証の失敗が多い
POSTメソッドの比率が高い端末
TCP443番以外のCONNECTメソッド
Content-Typeヘッダ値がコンテンツ内容と不一致
複数のUser-Agent値を使われている端末
User-Agentがレアな値
Hostヘッダ値がIPアドレス（IPアドレス直打ち）
自己署名証明書を使ったHTTPS通信
300番台、400番台のステータスコードが多いサイト
実行ファイルのダウンロード（exe、dll、sys、、、）
URLが長い
クラウドストレージへのアクセス

DNS

通信先のドメイン年齢が若い
TLDがレア（.onion、.cn、.ru、、、）
DNS名前解決（No such name）の失敗が多い
DNSクエリーの回数が多い