解析事例（平成28年10月）

@police

～　Daserf　～
～　アジアのサイバー攻撃グループでの使用が疑われるボット　～

アジアのサイバー攻撃グループでの使用が疑われる　Daserf　の解析を行った。

Daserf　はHTTPで攻撃者が用意したサーバに接続し、命令を受信する型のボットであった。

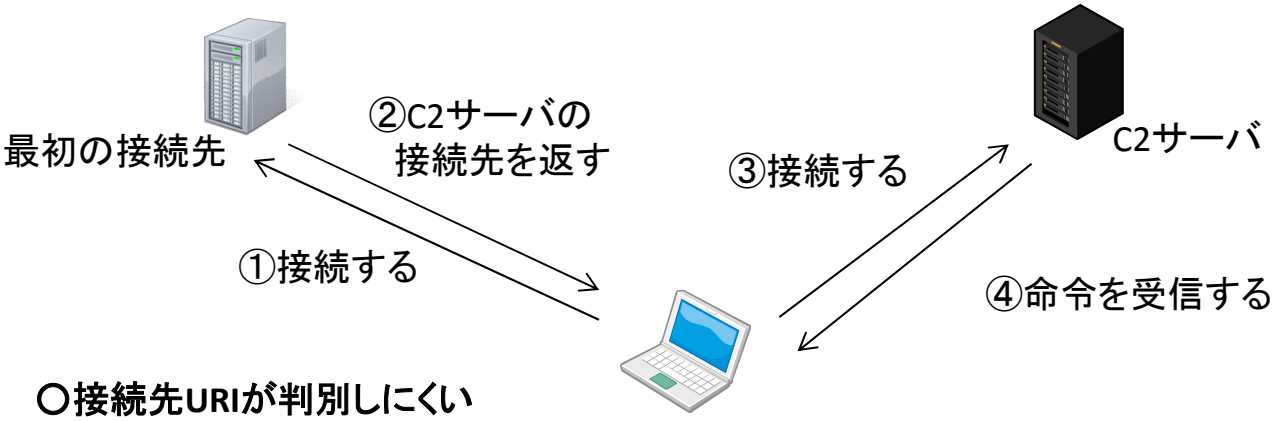
主な特徴としては次のようなものがある。

・検体内には最初の接続先しか設定しておらず、C2サーバの特定が困難

・接続先URIが判別しにくい

〇C2サーバの特定が困難

Daserf　は検体内に最初の接続先しか設定されていない。攻撃者とのやり取りを行うC2サーバの接続先は、最初の接続先から応答があった場合、その応答内にあるため、検体の解析のみではC2サーバの特定が困難である。



〇接続先URIが判別しにくい

Daserf　の接続先は毎回変化する。検体の固定値をランダムな値を使用して生成する。固定値を「md」とすると、「XXmdXXX.php」（ここで、「X」はアルファベット１文字を表す。）となる。例えば「kemdaor.php」や「oqmdnza.php」となる。そのため、URIが判別しにくくなっている。

〇ボット機能

・端末の情報収集（ドライブ、ファイル　等）　・ファイルのアップロード　・ファイルのダウンロード　・ファイルの実行

・ファイル操作（削除、作成　等）　・待機

〇その他の特徴

・通信内容の暗号化に変形base64テーブルを使用している

・Delphiで作成されている