解析事例(平成27年12月)

@police

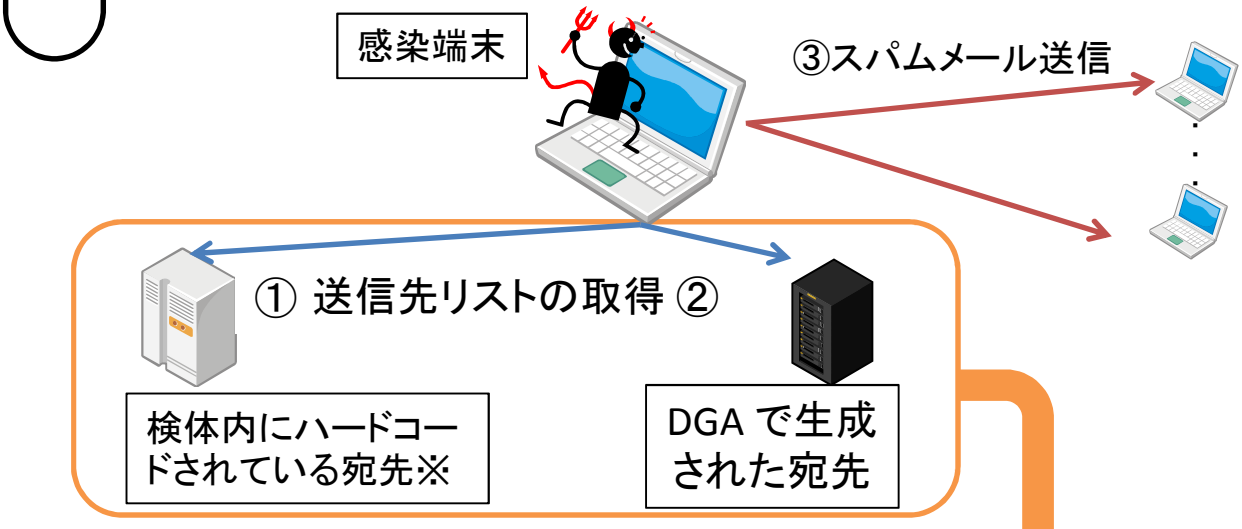
～　検体の解析だけでは目的の接続先が不明な検体　～

～　DGAを搭載したスパムボット　～

この不正プログラムは、まず最初に攻撃者が用意した送信先リストを取得するために外部ネットワークへの接続を試みる。送信先リストを入手できた場合に、そのリスト宛てにスパムメールを送信するといった機能を有している。

通信の流れは、検体内にハードコードされている宛先に接続し、有効な応答がない場合にDGA（Domain Generation Algorithm = 接続先のドメインを生成するアルゴリズム）を使用して生成した宛先に接続を行う。この際の通信内容は、動的解析及び静的解析の結果、すべて同様である。

このことから、応答があった宛先こそが目的の接続先であり、検体の解析では攻撃者の用意した送信先のリストの場所を特定することは困難となり、従来のブラックリスト方式のみでは防ぎきることが難しい。



※検体にハードコードされている宛先だけでも約100件が確認されている。

すべて同様の通信内容のため、検体の解析だけでは目的の接続先が分からない！