2016 年 2 月 5 日
株式会社セキュアソフト

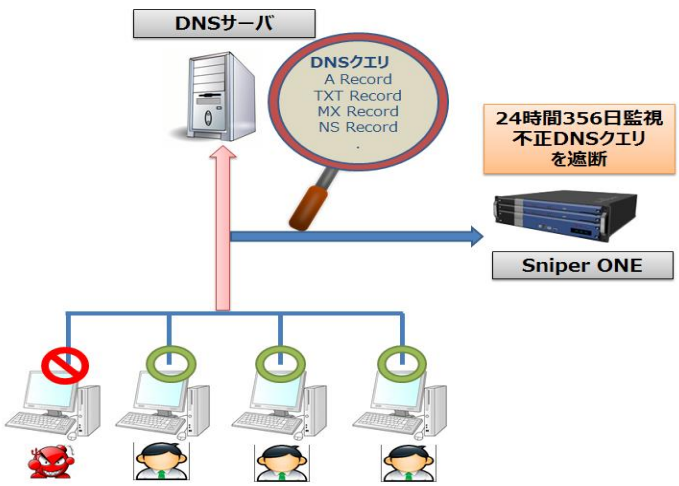
DNS で遠隔操作されるマルウェアの感染に対する注意喚起

攻撃対象を遠隔操作するマルウェアが攻撃を実行する際に DNS プロトコルを悪用しているケースがあると複数メディアで発表されています。弊社では、DNS の脆弱性を悪用する攻撃や DDoS 攻撃に対する注意喚起、それらの攻撃に対応する Sniper ONE の Anti-DDoS 機能や DNS 対策機能について以下のレポートでご案内いたしました。

「過去のレポート」
・2015 年 8 月 TR15-011_SecureSoft Sniper ONE による DoS・DDoS 攻撃対策例
・2015 年 11 月 TR15-014_注意喚起_日本国内で DDoS 攻撃によるウェブサービス被害が増加中
・2015 年 12 月 TR15-015_Securesoft Sniper ONE の特徴：DNS サーバの保護機能

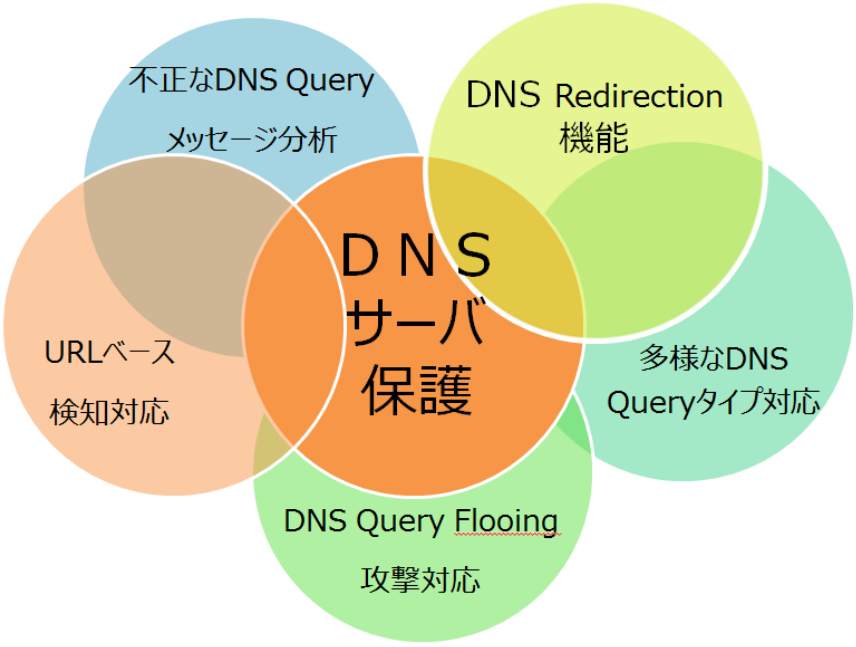
今回、発表された攻撃は DNS TXT Record に特定のデータを挿入し、C&C サーバが PC をリモートでコントロールする不正コードです。 DNS (Domain Name System) は、ドメイン名（コンピュータを識別する名称）を IP アドレスに自動的に変換するアプリケーション層プロトコルです。 DNS プロトコルで取り扱う DNS Record には幾つかの種類がありますが、DNS TXT Record はホスト名に関連付けるテキスト情報（文字列）を定義するレコードです。自ドメインの送信を許可するメールサーバの指定に SPF Record を使いますが、このレコードは DNS TXT Record に記載をします。その DNS TXT Record には C&C サーバとなる DNS の情報が記録されており、その DNS 情報を参照するクライアントはマルウェアのダウンロード先となる IP アドレスに接続され、マルウェアに感染してしまう被害が発生します。

このような DNS の特性を悪用する攻撃からシステムを守るためには、DNS クエリの中にどの様な情報が発生するのか、その情報をリアルタイムで検知し、収集したログから通信内容を把握して今後の対応を早期に立てる必要があります。



「図 1」24 時間 356 日監視で不正 DNS クエリを遮断

Sniper ONE の DNS 機能は様々な DNS　Record 種類の通信を検知する多数のシグネチャを持っています。そして、被疑対象となるパケット解析を実現する RawData 機能を有効化することで、詳細な解析と迅速な対応に役立ちます。



【図 2】SniperONE の DNS オプション機能（DNS サーバ保護対策）

以上