2015 年 12 月 11 日
株式会社セキュアソフト

Securesoft Sniper ONE の特徴：DNS サーバの保護機能

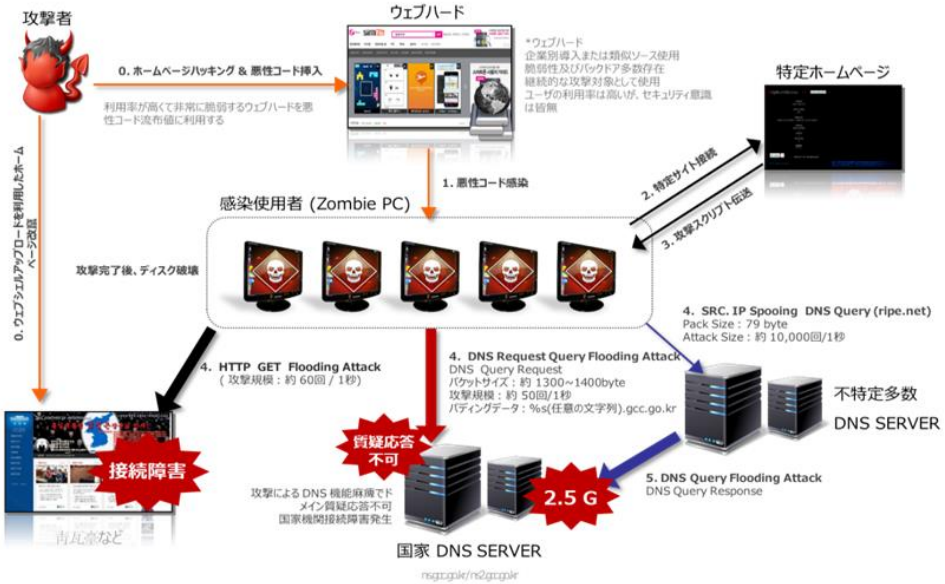
弊社が次世代型セキュリティアプライアンスとして提案している Sniper ONE には 8 つの目的に合わせた特徴的な機能が搭載されています。その 8 つの機能は、「IPS 機能」、「DDoS 対応機能」、「DNS サーバの保護機能」、「RegEx 対応機能」、「Rate Limit 機能」、「DHCP サーバの保護機能」、「VoIP ネットワークの保護機能」、「HTTPS 対応機能」となります。これらは Sniper ONE では、オプションライセンス化され、1 台のアプライアンスで 8 つの機能を組み合わせて利用する事が可能です。

本レポートでは Sniper ONE の 8 つの機能のうち、「DNS サーバの保護機能」について説明いたします。

1. 過去 DNS 攻撃の被害

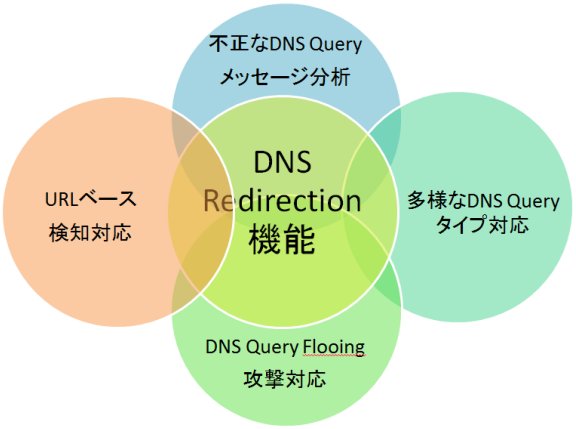
DNS 攻撃の実例については"【図 1 】DNS DDoS 攻撃の被害"の様に、攻撃者はファイル共有サービス「ウェブハード」をハッキングして悪性コードを埋め込みます。このサイトにアクセスした際に一般ユーザの PC は悪性コードに感染します。悪性コードに感染した PC は特定ホームページから攻撃用スクリプトがダウンロードされます。攻撃用スクリプトがインストールされた一般ユーザの PC を Zombie 化し、不特定多数の DNS サーバに対して送信元の IP を偽装した DNS クエリの送信を行います。DNS クエリの送信を受けた不特定多数の DNS サーバは、名前解決のため上位国家 DNS サーバに大量の DNS クエリを送信しました。その結果、上位国家 DNS サーバは正常なサービス停止する被害が発生しました。さらに Zombie 化された多数の PC は上位国家 DNS サーバに大量の DNS 攻撃が行い、その被害がより大きくなる事態が発生しました。攻撃完了後に Zombie 化された多数の PC のディスクも破損し、一般ユーザ側にも被害が発生しました。

DNS サービスが円滑に運用されない場合、インターネットのウェブサイトへの接続が遅くなるか、もしくはサイトに接続が出来なくなる事で、サービスを提供している企業やサービスを利用するユーザに大きな悪影響を与えることになります。



【図 1】DNS DDoS 攻撃の被害

2. Sniper ONE の DNS サーバの保護機能の特徴



【図 2】DNS サーバの保護機能の特徴

1)不正な DNS Query メッセージの検知・防御

IPS 機能と組み合わせて、シグネチャマッチングにより DNS パケットの中に不正メッセージがある場合に検知・防御する事が可能です。

2)URL ベースによる検知・防御

URL 情報を登録し、対象が明確に検知・防御します。本機能により、誤検知によるサービス中断の減少が可能です。（不正 URL を自動抽出～自動登録する機能を搭載予定です。）

3)DNS Query タイプによる検知・防御

様々な DNS Query タイプ別に専用のシグネチャを用意し検知・防御を可能にします。

【図 3】対応 DNS Query タイプ

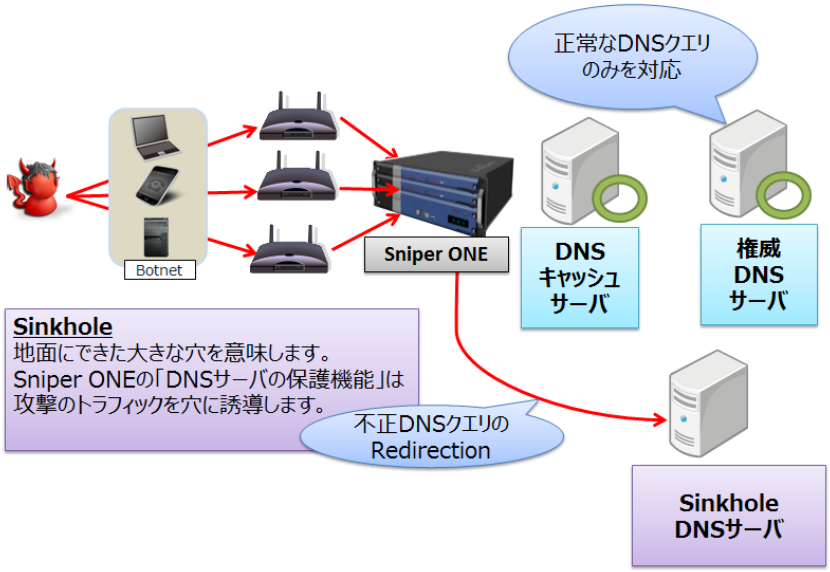
4)DNS Query Flooding 攻撃に対する検知・防御

送信元の IP を偽装した DNS Query Flooding 攻撃を検知・防御する事が可能です。

IP 別により DNS トラフィックを制御する事も可能です。

5）DNS Redirection 機能

DNS 攻撃を検知する場合は、正常な DNS キャッシュサーバや権威 DNS サーバではない Sinkhole DNS サーバに不正トラフィックを誘導し、正常な DNS サービスを保護する機能です。



【図 4】DNS Redirection 機能

3. まとめ

DNS 攻撃の最善な対策としては運用している DNS サーバを安全な領域に設置する事、サーバの脆弱性をチェックして Open Resolver の状態とならないように管理する事が重要です。しかし、管理する DNS サーバの数が多くなり、DNS のクエリが多い状況では簡単に管理・対応出来ない事が実際の課題です。そのために DNS に関する専門のセキュリティソリューションを投入する必要性が高まっています。

Sniper ONE の「DNS サーバの保護機能」を利用すると効果的に DNS サーバを様々な DNS 攻撃から保護する事が可能です。Sniper ONE の特徴である各機能の組み合わせを利用して、「DDoS 対応機能」、「IPS 機能」をセットにすることで、より高度化された DNS 攻撃に対応する事も可能となります。

本レポートでは「DNS サーバ保護機能」について簡単に説明していますが、より詳細な内容に関してお問い合わせをご希望される場合は、メールもしくがお電話でお問い合わせをお願い致します。

「お問い合わせ先」
E-mail: tech@securesoft.co.jp
電話番号：03-5464-9966

以上