2014 年 8 月 26 日
株式会社セキュアソフト

DNS 通信を使った DDoS 攻撃に関する注意喚起

2014 年 4~6 月頃、警察庁をはじめ、各セキュリティ機関から注意喚起をされている DNS 通信を使った DDoS 攻撃が多発し、弊社に対するお問合せも急増いたしました。DDoS 攻撃の特性上またいつ、どこで発生するかわからない状況です。早期に DDoS 対策を講じることを強くお勧めいたします。

攻撃の方法としては、各機関から公開されている以下のものを観測しております。

（１）「DNS リフレクション攻撃（DNS アンプ攻撃）」
（２）「オープンリゾルバ」を踏み台に利用した DDoS 攻撃

弊社で観測した攻撃の特徴としては、発信元をヨーロッパ圏の IP アドレスに偽装した多数のアドレスから ISP 等のサービス事業者が所有する DNS サーバー宛に大量に問合せするというものでした。1 つ 1 つの問合せパケットについては帯域幅を枯渇させたり、サーバーの処理負荷を重くするような効果は無く、問い合わせ内容もシンプルですが、発信元アドレスと問い合わせ内容（サブドメイン）をランダムに変化させながら数十万 PPS におよぶ大量の問合せをおこないサーバーの応答リソースを枯渇させました。実際には存在しない FQDN のサブドメイン部をランダムに変化させながら問い合わせし、一見規則性の無いランダムな発信元 IP アドレスにする等、攻撃プログラムの巧妙化がすすんでいると推測されます。

DNS サーバーに対する DDoS 攻撃の対策として「オープンリゾルバ」の根絶が理想ですが、一般家庭等で運用されているブロードバンドルータ等も含まれるため早期解決は難しい状況です。各機関から対応策が公開されておりますので、まずお使いのシステムにおける対策を早急に行われることをお勧めいたします。なお、SecureSoft Sniper シリーズでは DNS 通信の DDoS 攻撃に対する検知機能とサーバーのキャパシティを超える負荷を軽減させる機能を搭載しており、今回の攻撃に対する DNS サーバーの防御方法の 1 つとしてご活用いただくことが可能です。

以上