【Technical Report 14-004】
新機能

2014 年 12 月 5 日
株式会社セキュアソフト

Securesoft Sniper ONE が「DNS 水責め攻撃」対策に対応

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された DNS 通信を使った DDoS 攻撃が多発しました。本年のネットワークセキュリティインシデントにおいて大変重大な被害を及ぼし、また現在もこの攻撃についてはインターネット上で増加の一途をたどっています。弊社からも Technical Report 14-003 にてご報告いたしましたとおり、早期に DDoS 攻撃対策を講じることを今一度強くお勧めいたします。

最近の攻撃手法として注目されているのが、「DNS Water Torture（Slow Drip）攻撃」いわゆる「DNS 水責め攻撃」ですが、この攻撃手法の特徴は、マルウェアに感染した攻撃者の管理下にある大量の Bot 端末からそれぞれ少量の IP アドレス詐称した不正な DNS 問合せをおこなうことにあります。この攻撃の結果、権威 DNS サーバー並びに ISP 等のオープンキャッシュ DNS サーバーへの負荷がかかることで DNS サービスシステムが停止してしまい広範囲に影響が及びます。

セキュアソフトではこのような状況に対して、2014 年 12 月 24 日発売予定のセキュリティ統合プラットフォーム Securesoft Sniper ONE の DNS 攻撃対策オプション機能に「DNS 水責め攻撃」対策機能を搭載することを決定いたしました。「DNS 水責め攻撃」については一般的に通信の緩和法や問合せ遮断などの手法が知られておりますが、いずれもシステム管理者の非常に負担の思い運用作業があって成り立ちます。今回の Securesoft Sniper ONE では、ランダムなサブドメイン名の DNS 問合せ結果から判断される不正な問合せ内容を DNS Query 識別機能に反映し不正な通信を識別・制御可能な DNS 攻撃専用対策機能や UDP DDoS トラフィックの Mitigation をおこなう Anti-DDoS 機能などで対応し、「DNS 水責め攻撃」対策を実現いたします。

以上