2016 年 1 月 8 日

株式会社セキュアソフト

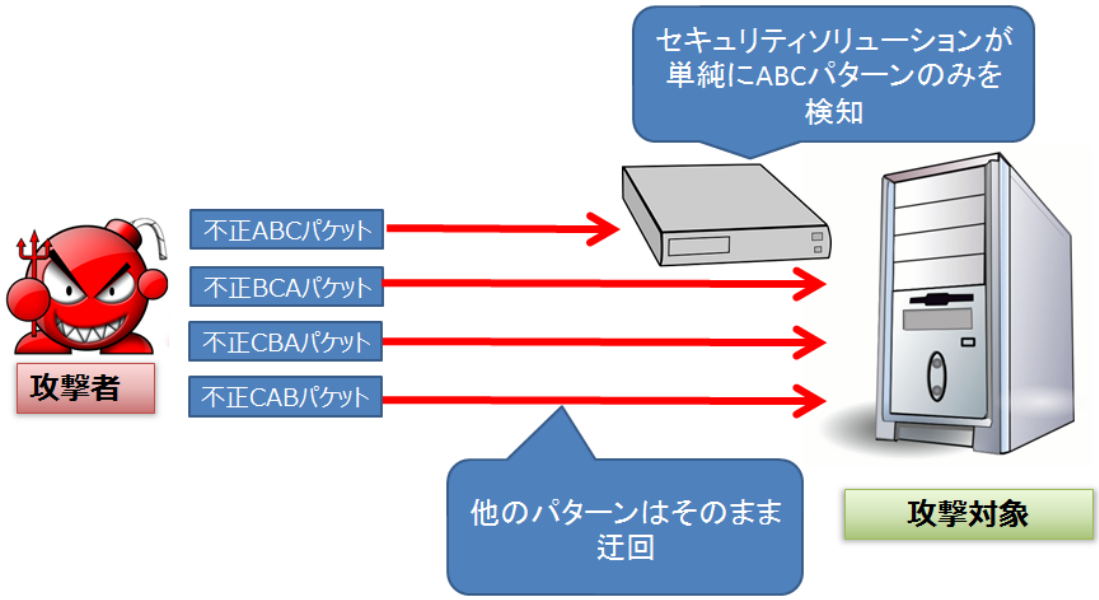
Securesoft Sniper ONE の特徴：Regular Expression 機能

Sniper ONE には 8 つの特徴的なオプション機能が搭載されています。「IPS 機能」、「DDoS 対応機能」、「DNS サーバ保護機能」、「Regular Expression 機能」、「Rate Limit 機能」、「DHCP サーバ保護機能」、「VoIP ネットワーク保護機能」、「HTTPS 対応機能」があります。Sniper ONE はこのオプションライセンス機能を利用して 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 つの機能の中で「Regular Expression 機能」について説明いたします。

1. 高度化する攻撃パターン

近年、攻撃のパターンが高度化しているケースが多く検出されています。攻撃者は攻撃対象システムやネットワークに対して、1 つの攻撃パターンのみを利用すると相手のセキュリティソリューションによって簡単に遮断されることを考慮して、幾つかのパターンを生成することでセキュリティソリューションを迂回しようとします。その技巧としては、攻撃者の IP アドレス（送信元 IP アドレス）を様々に変更する、攻撃パケット送信量を不定期に増減する等の方法を利用します。さらに、攻撃パケット内のペイロード部を巧妙に変更させながら送信する方法も利用することが多くなっています。インターネットに多く配布されている高度化された攻撃ツールを利用して、専門知識を持ってない人でも容易にこのような多様な攻撃を実現する事ができる状況となっています。



【図 1】多様な攻撃パターンによって攻撃を迂回

2. Sniper ONE の Regular Expression オプション機能の特徴

Sniper ONE は「Regular Expression 機能」を利用する事によって、Regular Expression（正規表現式）の記述で、高度化する攻撃を検知及び遮断することができます。Regular Expression 文法はセキュリティ運用上に広く使われる共通文法のため、多様なネットワークの脅威に対し、対応することが可能です。さらに、ネットワークシステムの特性を理解しているユーザが Regular Expression（正規表現式）シグネチャを定義・チューニングすることによってシステムの特性を反映した精巧なシグネチャを利用することができます。また、柔軟性の高い記述設定により 1 個のポリシーで多様な攻撃パターンに対応することも可能です。

■Regular Expression シグネチャの例

```
alert tcp any any -> any 80 ( content:"GET";pcre:"/math_sum.mscgi¥?a=AAAA/";)
```

Sniper ONE では Sniper CERT からの推奨 Regular Expression 文法のシグネチャ提供を準備しており、ユーザがより簡単に運用が出来るようにサポートする予定です。又、ユーザ定義によりユーザが個別にパターンを登録する機能もサポートします。

3. まとめ

多様化するサイバー攻撃に対応するためには大量のシグネチャを準備する必要があります。攻撃パターンが様々に変化することで、誤検知率が高まる可能性もあります。さらに、検知量が多くなる事によって攻撃の分析に手間が掛かるなどの影響も考えられます。Sniper ONE の Regular Expression 機能は Regular Expression（正規表現式)記述設定の活用により、検知率を高め、且つ効率的にシグネチャを設定できるため、攻撃への対策・分析に役立ちます。

以上