2016 年 1 月 22 日
株式会社セキュアソフト

Securesoft Sniper ONE の特徴：HTTPS 対応機能

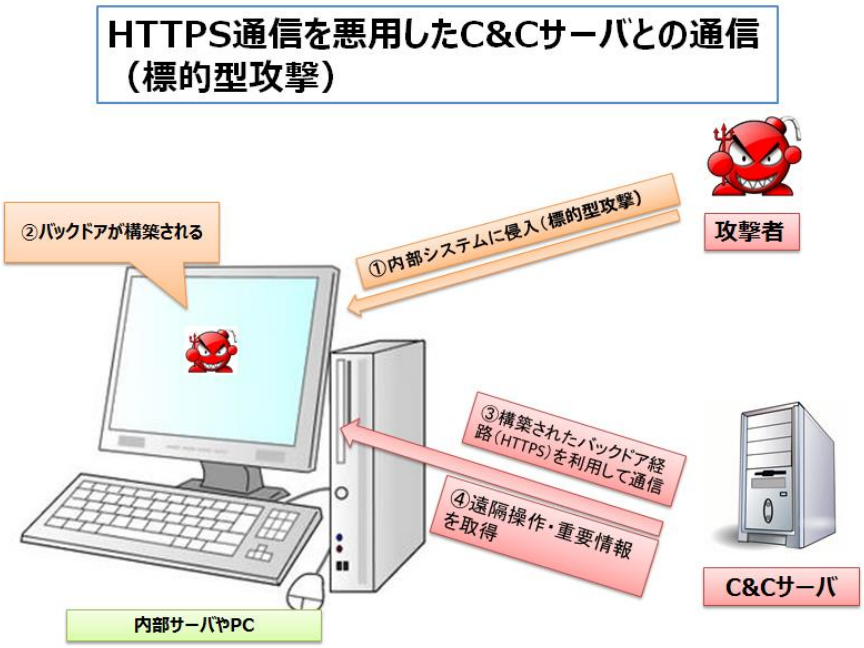
Sniper ONE には 8 つの特徴的な機能が搭載されています。「IPS 機能」、「DDoS 対応機能」、「DNS サーバの保護機能」、「Regular Expression 対応機能」、「Rate Limit 機能」、「DHCP サーバの保護機能」、「VoIP ネットワークの保護機能」、「HTTPS 対応機能」があります。Sniper ONE はこのオプションライセンス機能を利用して 1 台のアプライアンスで 8 つの機能を組み合わせて利用する事が可能です。

本レポートでは Sniper ONE の 8 つの機能の中で「HTTPS 対応機能」について説明いたします。

1. HTTPS 通信を悪用したサイバー攻撃による被害

HTTPS（Hypertext Transfer Protocol Secure）は、HTTP による通信を安全に行うためのプロトコルです。SSL/TLS プロトコルによる接続で、暗号化された HTTP 通信を行うことを HTTPS と呼んでいます。暗号化された通信により安全が確保されますが、攻撃に利用されると検知が難しくなります。

図 1 は攻撃者が SSL プロトコルを利用したサイバー攻撃の例となります。攻撃者は標的型攻撃を実行するとき、組織内ネットワークに侵入し、外部の C&C サーバとの通信を行って重要情報を盗み出していきます。外部の C&C サーバとの通信の際に SSL 通信を利用します。たとえば、HTTPS で保護されたサイトからドライブバイダウンロード攻撃や、C&C サーバへの通信に smtps や https などを使用し、SSL 通信の検査に対応しないセキュリティ製品の監視を回避し、情報を取得します。



【図 1】HTTPS 通信を悪用した C&C サーバとの通信

2. Sniper ONE の HTTPS 対応機能

Sniper ONE の HTTPS 対応機能はサーバ情報とポート情報を Sniper ONE に登録する事で、保護対象サーバと接続しているクライアント（C&C サーバなどの悪意ある端末も含まれる）の間で HTTPS セッションが結ばれている場合に、通信時間、通信量(byte, packet)等の情報をリアルタイムに表示可能です。

また、HTTPS の暗号化された通信による攻撃を検知及び防御することも可能です。Sniper ONE に保護対象サーバの Private Key を登録する事で、該当サーバに対して発生する SSL セッションを検知する事が可能です。Sniper ONE の HTTPS 対応機能は HTTPS のデフォルトポートである 443 ポートだけではなく、任意のポートを登録する事で Private な HTTPS ポートについても柔軟に対応する事が可能です。

Sniper ONE の HTTPS 対応機能がサポートする Private Key Type 及び File Format は下表となります。
（2016 年 1 月時点）

[表 1]サポート可能なPrivate Key及びFile Format

Version	PKCS Type	File Format	暗号化有無	Sniper ONE サポート可否
0.1.0	**PKCS #1**	PEM	PlainText	O
		DER	PlainText	O
	PKCS #5	PEM	ciphertext	O
	PKCS #8	PEM	PlainText	O
		DER	PlainText	O
		PEM	ciphertext	O
		DER	ciphertext	O
	PKCS #12	.p12	ciphertext	X
		.pfx	ciphertext	X

3．まとめ

HTTPS 通信を悪用するサイバー攻撃から組織のインフラを守るためには HTTPS 通信をリアルタイムに監視できる対策が必要です。Sniper ONE の HTTPS 対応機能は、保護対象のサーバで発生する HTTPS 通信を 24 時間 365 日監視し、サイバー攻撃や重要情報流出のモニタリングや保護ができます。

HTTPS 通信を悪用した攻撃は増加することが予想されます。Sniper ONE の HTTPS 対応機能は簡単に利用することが可能です。本機能を利用して HTTPS 通信をモニタリングし、攻撃を検知・遮断することで重要情報の保護が可能となります。

以上